

# INDUSTRY SPEAKS ON CYBERSECURITY

---

## HEARING OF THE SUBCOMMITTEE ON CYBERSECURITY, SCIENCE AND RESEARCH, AND DEVELOPMENT BEFORE THE SELECT COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES ONE HUNDRED EIGHTH CONGRESS FIRST SESSION

JULY 15, 2003

**Serial No. 108-16**

Printed for the use of the Select Committee on Homeland Security



Available via the World Wide Web: <http://www.access.gpo.gov/congress/house>

U.S. GOVERNMENT PRINTING OFFICE

97-672 PDF

WASHINGTON : 2004

---

For sale by the Superintendent of Documents, U.S. Government Printing Office  
Internet: [bookstore.gpo.gov](http://bookstore.gpo.gov) Phone: toll free (866) 512-1800; DC area (202) 512-1800  
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

## SELECT COMMITTEE ON HOMELAND SECURITY

CHRISTOPHER COX, California, Chairman

JENNIFER DUNN, Washington	JIM TURNER, Texas, Ranking Member
C.W. BILL YOUNG, Florida	BENNIE G. THOMPSON, Mississippi
DON YOUNG, Alaska	LORETTA SANCHEZ, California
F. JAMES SENSENBRENNER, JR., Wisconsin	EDWARD J. MARKEY, Massachusetts
W.J. (BILLY) TAUZIN, Louisiana	NORMAN D. DICKS, Washington
DAVID DREIER, California	BARNEY FRANK, Massachusetts
DUNCAN HUNTER, California	JANE HARMAN, California
HAROLD ROGERS, Kentucky	BENJAMIN L. CARDIN, Maryland
SHERWOOD BOEHLERT, New York	LOUISE MCINTOSH SLAUGHTER, New York
LAMAR S. SMITH, Texas	PETER A. DeFAZIO, Oregon
CURT WELDON, Pennsylvania	NITA M. LOWEY, New York
CHRISTOPHER SHAYS, Connecticut	ROBERT E. ANDREWS, New Jersey
PORTER J. GOSS, Florida	ELEANOR HOLMES NORTON, District of Columbia
DAVE CAMP, Michigan	ZOE LOFGREN, California
LINCOLN DIAZ-BALART, Florida	KAREN McCARTHY, Missouri
BOB GOODLATTE, Virginia	SHEILA JACKSON-LEE, Texas
ERNEST J. ISTOOK, JR., Oklahoma	BILL PASCRELL, JR., New Jersey
PETER T. KING, New York	DONNA M. CHRISTENSEN, U.S. Virgin Islands
JOHN LINDER, Georgia	BOB ETHERIDGE, North Carolina
JOHN B. SHADEGG, Arizona	CHARLES GONZALEZ, Texas
MARK E. SOUDER, Indiana	KEN LUCAS, Kentucky
MAC THORNBERRY, Texas	JAMES R. LANGEVIN, Rhode Island
JIM GIBBONS, Nevada	KENDRICK B. MEEK, Florida
KAY GRANGER, Texas	
PETE SESSIONS, Texas	
JOHN E. SWEENEY, New York	

JOHN GANNON, *Chief of Staff*

UTTAM DHILLON, *Chief Counsel and Deputy Staff Director*

DAVID H. SCHANZER, *Democrat Staff Director*

MICHAEL S. TWINCHEK, *Chief Clerk*

---

## SUBCOMMITTEE ON CYBERSECURITY, SCIENCE, AND RESEARCH & DEVELOPMENT

MAC THORNBERRY, Texas, Chairman

PETE SESSIONS, Texas, Vice Chairman	ZOE LOFGREN, California
SHERWOOD BOEHLERT, New York	LORETTA SANCHEZ, California
LAMAR SMITH, Texas	ROBERT E. ANDREWS, New Jersey
CURT WELDON, Pennsylvania	SHEILA JACKSON-LEE, Texas
DAVE CAMP, Michigan	DONNA M. CHRISTENSEN, U.S. Virgin Islands
ROBERT W. GOODLATTE, Virginia	BOB ETHERIDGE, North Carolina
PETER KING, New York	CHARLES GONZALEZ, Texas
JOHN LINDER, Georgia	KEN LUCAS, Kentucky
MARK SOUDER, Indiana	JAMES R. LANGEVIN, Rhode Island
JIM GIBBONS, Nevada	KENDRICK B. MEEK, Florida
KAY GRANGER, Texas	JIM TURNER, Texas, <i>ex officio</i>
CHRISTOPHER COX, CALIFORNIA, <i>ex officio</i>	

# CONTENTS

	Page
STATEMENTS	
The Honorable Mac Thornberry, Chairman, Subcommittee on Cybersecurity, Science, and Research & Development, and a Representative in Congress From the State of Texas .....	1
The Honorable Christopher Cox, Chairman, Select Committee on Homeland Security, and a Representative in Congress From the State of California .....	45
The Honorable Jim Turner, Ranking Member, Select Committee on Homeland Security, and a Representative in Congress From the State of Texas .....	62
The Honorable Robert E. Andrews, a Representative in Congress From the State of New Jersey .....	58
The Honorable Donna M. Christensen, a Delegate in Congress From the U.S. Virgin Island .....	47
The Honorable Bob Etheridge, a Representative in Congress From the State of North Carolina .....	45
The Honorable Sheila Jackson-Lee, a Representative in Congress From the State of Texas .....	54
The Honorable Zoe Lofgren, a Representative in Congress From the State of California .....	1
The Honorable Loretta Sanchez, a Representative in Congress From the State of California .....	52
The Honorable Pete Sessions, a Representative in Congress From the State of Texas .....	49
The Honorable Lamar S. Smith, a Representative in Congress From the State of Texas .....	40
WITNESSES	
Mr. Jay Adelson, CTO & Founder, Equinix, Inc.	
Oral Statement .....	18
Prepared Statement .....	20
Mr. Whitfield Diffie, Chief Security Officer Sun Microsystems, Inc.	
Oral Statement .....	8
Prepared Statement .....	10
Ms. Tatiana Gua, Chief Trust Officer and Senior Vice President, America On-Line (AOL) Core Services, AOL Time Warner	
Oral Statement .....	28
Prepared Statement .....	30
Mr. Frank Ianna, President—AT&T Network Services, AT&T Corporation	
Oral Statement .....	22
Prepared Statement .....	24
Dr. James Craig Lowery, Chief Security Architect/Software Architect and Strategist, Dell Computer Corporation	
Oral Statement .....	14
Prepared Statement .....	16
Mr. Phil Reitinger, Senior Security Strategist, Microsoft Corporation	
Oral Statement .....	2
Prepared Statement .....	4
APPENDIX	
MATERIALS SUBMITTED FOR THE RECORD	
Responses to Questions for the Record from Dr. James Craig Lowery .....	72

#### IV

	Page
Responses to Questions for the Record from Mr. Jay Adelson .....	72
Responses to Questions for the Record from Mr. Frank Ianna .....	74
Responses to Questions for the Record from Ms. Tatiana Gau .....	78
Responses to Questions for the Record from Mr. Phil Reitingen .....	79

## INDUSTRY SPEAKS ON CYBERSECURITY

---

TUESDAY, JULY 15, 2003

U.S. HOUSE OF REPRESENTATIVES  
SUBCOMMITTEE ON CYBERSECURITY, SCIENCE  
AND RESEARCH AND DEVELOPMENT  
SELECT COMMITTEE ON HOMELAND SECURITY,  
Washington, D.C.

The subcommittee met, pursuant to call, at 10:02 a.m., in Room 2118, Rayburn House Office Building, Hon. William Thornberry [chairman of the subcommittee] presiding.

Present: Representatives Thornberry, Sessions, Boehlert, Smith, Camp, Linder, Lofgren, Sanchez, Andrews, Jackson Lee, Christensen, Etheridge, Lucas, Langevin, Meek, Cox (*ex officio*), Turner (*ex officio*), also present, Dunn.

Mr. THORNBERRY. [Presiding.] The hearing will come to order.

This hearing of the Subcommittee on Cybersecurity, Science, Research & Development will take testimony today on industry perspectives on cybersecurity.

And let me first thank each of the witnesses for making the effort to be here today. As you look down the line, it is truly not only a group that has a lot to offer to this subcommittee, but the world leaders in so many fields.

So I appreciate each of you being here, and I appreciate the staff being able to assemble this panel and all we have, and enable us to learn from it.

Ms. Lofgren and I again ask unanimous consent that members other than the chairman and ranking member waive oral written statements—oral opening statements, written opening statements will be made part of the record and each of the witnesses written statements will also be made a part of our record.

And at this time the Chair will yield to the distinguished gentlelady from California, Ranking Member Ms. Lofgren.

Ms. LOFGREN. Thank you, Mr. Chairman.

This is a terrific panel and I know that we at the end of the day will know more about what we face as a nation in the area of cybersecurity and will have, I think, a better idea of the prudent steps that we should take.

I am especially pleased—I mean, every one of the witnesses is spectacular—but I would like to issue a special welcome to Whit Diffie, who was part of the encryption wars that Mr. Goodlatte and I engaged in with so many of the members of the committee a few years ago, and the inventor of public key encryption.

I hope that as we hear from the witnesses, we can particularly hear about your company's investment into research and develop-

ment on cyber vulnerabilities, and without going into specifics, learn about the various types of cyber attacks your company has faced in the past year, your company's policies on information-sharing relative to cyber attacks as well as any experience you have had in dealing with the Department of Homeland Security.

As the chairman and I have discussed in past occasions, I think we all know the issue really is what benchmarks do we put in place, how do we audit or ensure benchmarks are being met, and which carrot and stick do we put in place.

And those are broad categories, but the details are troublesome.

And so that is what we are, I think, dealing with and we know that most of the infrastructure that needs to be protected is in the private sector, so it is absolutely so important that you are here today.

And I would ask—well, we already have consent to put my full statement into the record.

And I thank the chairman for yielding.

Mr. THORNBERRY. Thank you, gentlelady.

And I think we see things exactly the same.

We are not going to be successful as a country without a partnership with each of you and other industry folks.

So at this time I want to turn to our witnesses.

As I mentioned, your full written statement will be made part of the record, and I will invite each of you to either summarize it or make such comments as you wish.

We are going to go down the row.

And I am going to start with Philip Reitingger, who is senior security strategist with Microsoft.

Thank you for being here with us today.

And you are recognized for five minutes.

#### **STATEMENT OF MR. PHIL REITINGER, SENIOR SECURITY STRATEGIST, MICROSOFT CORPORATION**

Mr. REITINGER. Thank you very much.

Good morning.

Good morning, Chairman Thornberry, Ranking Member Lofgren, and members of the subcommittee.

As the chairman indicated, my name is Phillip Reitingger, and I am a senior security strategist with Microsoft Corporation.

I want to thank you for the opportunity to appear before you here today to provide our views on an issue that affects government, businesses and consumers—cybersecurity. Microsoft is deeply committed to confronting the challenges of cybersecurity and we recognize our responsibility to make our products ever more secure.

Our efforts accelerated after September 11 and crystallized when Bill Gates launched our trustworthy computing initiative in January 2002. Trustworthy computing is Microsoft's top priority and involves every aspect of the company. Last year, we had all 8,500 developers on the Windows team stop developing new code to focus on security. We spent over two months training our developers, reviewing the security of existing codes, reducing potential vulnerabilities, modeling threats, and conducting penetration testing of the code. This critical investment cost us an estimated \$200

million dollars and delayed by months the release of our recent Windows Server 2003 product.

Trustworthy computing, broadly, means that we are working to ensure that computers better protect the security of personal and corporate information, enable people in organizations to control how their information is used, and are more reliable. Security, privacy, reliability and business integrity are the core pillars of our trustworthy computing initiative. In this effort, we are working to create products and services that are secure by design, secure by default, secure in deployment, and to communicate openly about security.

Secure by design means two things. Writing more secure code and architecting more secure products and services. Secure by default means writing computer software that is secure out of the box, whether in a home environment or an IT department. Secure in deployment means making it easier for consumers and IT professionals to maintain the security of their systems. And communications means sharing what we have learned, both within and outside of Microsoft, particularly through our industry-leading response center.

The trustworthy computing goals are ingrained in our culture and are part of the way we value our work. Yet, we recognize that trustworthy computing and improved cybersecurity will not result from the efforts of one company alone. As demonstrated by my colleagues on this panel, we are not alone in these efforts. Microsoft is dedicated to working together with these industry partners and with government leaders to make the goals of trustworthy computing an industry-wide reality.

We do so in a number of forums, including the IT ISACs, the Partnership for Critical Infrastructure Security, the National Cybersecurity Alliance and the Trusted Computing Group. We also recognize that technology, alone, cannot provide a complete answer.

I want to outline a few specific areas where government policy can help promote cybersecurity. First, the government can help by recognizing IT products engineered for security and by securing its own systems. This can include purchasing common-criteria certified products, and even awarding a Malcolm Baldrige type of award for security solutions.

Secondly, we support additional federal funding for cybersecurity research development, including university-driven research that can be transferred to the private sector so that industry can further develop this technology and deploy it widely.

Third, we support an international law enforcement framework that establishes minimum criminal liability and penalty rules for cyber crime, so that cyber attackers cannot escape punishment for attacks against the United States by seeking refuge outside our borders.

Fourth, the government must be both a provider as well as a consumer of valuable threat information.

Finally, even with the creation of the Department of Homeland Security and the National Cybersecurity Division, both of which Microsoft supported, cybersecurity remains an interagency problem. Without a multi-disciplinary effort by both government and industry, we will not succeed.

In conclusion, Microsoft is committed to strengthening the security of our products and services and is equally committed to working with governments and our industry peers on security issues.

In the end a coordinated response to cybersecurity risks offers the greatest hope for promoting security and fostering the growth of a vibrant online economy. Thank you very much.

[The statement of Mr. Reitingger follows:]

#### PREPARED STATEMENT OF MR. PHILIP REITINGER

Chainnan Thornberry, Ranking Member Lofgren, and Members of the Subcommittee: My name is Philip Reitingger, and I am a Senior Security Strategist at Microsoft reporting directly to Microsoft's Chief Security Strategist. I want to thank you for the opportunity to appear today to provide our views on an issue that affects governments, businesses, and consumers around the world—cybersecurity. It is the responsibility of all of us to ensure that the tremendous benefits of technology for governments, business and consumers are not thwarted by attacks on our computer systems. Because most cyber attacks are not discovered or, if discovered, are not reported, and because we have no national or international statistically rigorous measurement of damages from cyber crime, the exact cost of cyber attacks to companies and consumers is unknown. But four things are clear:

First, there are people in cyberspace who seek to corrupt our systems. These criminals act with the knowledge that they are highly unlikely to be caught, let alone prosecuted and imprisoned.

Second, the known damages are significant—perhaps in the billions of dollars annually. Software applications and operating systems, and the networks on which they reside, are ubiquitous and integral to society, and attacks upon them can cause significant disruption.

Third, as September 11th taught us, our preconceived notions of the risk from terrorism and other threats may underestimate the actual risk by orders of magnitude. A cyber attack on the backbone of one of our nation's critical information infrastructures could disrupt America's physical and economic well-being and have a massive worldwide impact.

Fourth, and most important, these attacks have an impact greater than immediate financial loss. Perhaps their greatest cost is the loss of consumer trust in information technology. Without such trust, society cannot realize the full potential of information technology. Thus, the effort to achieve cybersecurity—to achieve the trust necessary to reap the benefits of the digital age—is a critical priority for us all.

At Microsoft, we are deeply committed to cybersecurity and we recognize our responsibility to make our products ever more secure. We are at the forefront of industry efforts to enhance the security of computer programs, products and networks, and better protect our critical information infrastructures. We also work closely with our partners in industry, government agencies and law enforcement around the world to identify security threats to computer networks, share best practices, improve our coordinated response to security breaches, and prevent computer attacks from happening in the first place. These efforts accelerated after September 11 and crystallized when Bill Gates launched our Trustworthy Computing initiative in January 2002.

Today, I want to describe the ways in which we believe industry and government can work in partnership to promote cybersecurity. First, I will discuss our commitment to Trustworthy Computing and how it is reflected in our products and our research and development efforts. Next, I will discuss our efforts to join forces with industry and government to help guard against cyber-threats and enhance security for businesses and consumers. Finally, I will address government's critical and tailored role in enhancing cybersecurity.

#### **Microsoft's Commitment to Trustworthy Computing**

Trustworthy Computing is Microsoft's top priority and involves every aspect of the company. Last year, we had all 8,500 developers on the Windows team stop developing new code to focus on security. We spent over two months training our developers, reviewing the security of existing code, reducing potential vulnerabilities, modeling threats and conducting penetration testing of the code. This effort cost us an estimated \$200 million dollars, and delayed by months the release of our recent Windows Server 2003 product. But we know that it was worth these costs, and it was a critical step to enhance the security of Microsoft's key software platform.

“Trustworthy Computing” broadly means that we are working to ensure that computers better protect the security of personal and corporate information, enable people and organizations to control how their information is used, and are more reliable. We also are working to ensure that when problems do arise, they can be resolved immediately and predictably. Security, privacy, reliability and business integrity are the core pillars of our Trustworthy Computing initiative.

The security pillar of Trustworthy Computing is most relevant for today’s hearing. Under this pillar, Microsoft is working to create products and services that are Secure by Design, Secure by Default, and Secure in Deployment, and to communicate openly about security.

- “Secure by Design” means two things: writing more secure code and architecting more secure products and services. Writing more secure code means using a redesigned software development process that includes training for developers, code reviews, automated testing of code, threat modeling, and penetration testing. Architecting more secure products and services means designing products with built in and aware security, so that security imposes less of a burden on users and security features are actually used.
- “Secure by Default” means that computer software is secure out of the box, whether it is in a home environment or an IT department. It means shipping products to customers in a locked-down configuration with many features turned off, allowing customers to configure their systems appropriately, in a more secure way, for their unique environment.
- “Secure in Deployment” means making it easier for consumers and IT professionals to maintain the security of their systems. We have a role in helping consumers help themselves by creating easy-to-use security technology. Due to the complexity of software and multiple environments in which it may be placed, software will never be perfectly secure while also being functional. Accordingly, “secure in deployment” means providing training on threats and security; offering guidance on how to deploy, configure and maintain products securely; and providing better security tools for users, so that when a vulnerability is discovered, the process of patching that vulnerability is simple and effective.
- “Communications” means sharing what we learn both within and outside of Microsoft, providing clear channels for people to talk to us about security issues, and addressing those issues with governments, our industry counterparts, and the public.

The Trustworthy Computing goals are real and specific, and this effort is now ingrained in our culture and is part of the way we value our work. It is demonstrated by our enhanced software development process. It is demonstrated by our continued development of more sophisticated security tools, including threat models and risk assessments, to better identify potential security flaws in our products. It is demonstrated by our formation of what we believe to be the industry’s best security response center to investigate immediately any reported product vulnerability and build and disseminate the needed security fix. And perhaps more clearly than anything else, it is demonstrated by our delay in releasing a product for months to continue to improve its security. In short, security is—as it should be—a fundamental corporate value. We make every effort to address security in the initial product design, during product development, and before a product’s release, and we remain committed to security in the product once it has gone to market.

At times, of course, people worry that increased security may lead to an erosion of privacy. It is important to note that we do not view security and privacy as in inevitable conflict. In fact, we think technology can help protect both simultaneously. We hear repeatedly from customers that they need new ways to control how their digital information is used and distributed. In response, we are working on a number of emerging rights management technologies that will help protect many kinds of digital content and open new avenues for its secure and controlled use. For example, we are on the verge of releasing Microsoft Windows Rights Management Services (RMS), a premium service for Windows Server 2003 that works with applications to help customers protect sensitive web content, documents and e-mail. The rights protection persists in the data regardless of where the information goes, whether online or offline. In this way it allows ordinary users and enterprises to take full advantage of the functionality and flexibility offered by the digital network environment—from sharing information and entertainment to transacting business—while providing greater privacy and persistent protections.

Much work on Trustworthy Computing, however, remains ahead of us. One key piece of that work is the Next-Generation Secure Computing Base (NGSCB). This is an on-going research and development effort to help create a safer computing environment for users by giving them access to four core hardware-based features missing in today’s PCs: strong process isolation, sealed storage, a secure path to and

from the user, and strong assurances of software identity. These changes, which require new PC hardware and software, can provide protection against malicious software and enhance user privacy, computer security, data protection and system integrity. We believe these evolutionary changes ultimately will help provide individuals and enterprises with greater system integrity, information security and personal privacy, and will help transform the PC into a platform that can perform trusted operations, to the benefit of consumers.

#### **Microsoft's Collaboration with Third Parties on Security Initiatives**

Notwithstanding the robust nature of our own efforts, we recognize that Trustworthy Computing and improved cybersecurity will not result from the efforts of one company alone. And, as will be demonstrated by my colleagues from this and the next panel, we are not alone in these efforts—responsible information technology companies increasingly focus on security as a key corporate goal. Microsoft is dedicated to working together with these industry partners and with government leaders to make the goals of Trustworthy Computing an industry-wide reality. For example, as part of our work on NGSCB, we work with a variety of hardware and software partners to ensure that the PC platform has built-in protection against future viruses, threats from hackers, and unauthorized access to private information and digital property.

In April of this year, we joined four other industry partners (AMD, Intel, IBM and Hewlett-Packard) in establishing the Trusted Computing Group (TCG), a not-for-profit organization formed to develop, define, and promote open standards for hardware-enabled trusted computing and security technologies. The primary goal is to help users protect their information assets (data, passwords, keys, etc.) from external software attack and physical theft and to provide these protections across multiple platforms, such as servers, PDAs, and digital phones.

In addition to these efforts, Microsoft remains committed to a multi-disciplinary approach to security that extends beyond technical solutions and specifications. Early detection and warning of cybersecurity threats, public education on cybersecurity, incident response, and prosecution of cyber-crimes, among other things, are all key aspects of creating a more secure computing environment. In order to have effective prevention and response, there must be an emphasis on cooperation and information sharing. For this reason, we have been supporters of the National Cyber Security Alliance and the Partnership for Critical Infrastructure Security, and we work closely with government agencies and other industry participants on both an informational and operational level to prevent and investigate computer intrusions and attacks.

We also helped found the Information Technology - Information Sharing and Analysis Center (IT-ISAC) and provided its first president. The IT-ISAC coordinates information-sharing on cyber-events among information technology companies and the government. We continue to support and are working with other members to improve the IT-ISAC's efforts to coordinate among members, with the government, and with other ISACs. Such efforts are critical because this nation's infrastructures were and are designed, deployed, and maintained by the private sector. The interdependencies among infrastructure sectors mean that damage caused by an attack on one sector may have disruptive and perhaps devastating effects on other sectors. Voluntary information sharing and industry-led initiatives, supported by government cybersecurity initiatives, comprise an essential first line of defense against such threats.

We believe that the information sharing engendered to date by the IT-ISAC and other ISACs is an important step in enhancing public-private cooperation in combating cybersecurity threats. Yet, there remains room for progress and government and industry should continue to examine and reduce barriers to appropriate exchanges of information, and build mechanisms and interfaces for such exchanges. This effort must involve moving away from ad hoc exchanges and toward exchanges that are built into business processes. This will require working toward a common understanding of the information that is valuable to share, when and how such information should be shared, and the means by which shared information will be protected. The keystones are trust and value—if an information sharing “network” provides value and the participants trust it, then information will be shared. While the appropriate structure and form of this network are still evolving for both industry and government, we are eager to see a robust exchange of information on cybersecurity threats and will work with government, our industry partners, and with the ISAC community toward that goal.

#### **Where Government Policy Can Make a Difference**

While the sorts of technology-related steps outlined above can address many of the security challenges we face, technology alone cannot provide a complete answer. A comprehensive response to the challenges of cybersecurity depends on both tech-

nology and public policy—and critically, on how technology and policy interact with and complement one another. I want to outline a few specific areas where government policy can be particularly helpful in promoting cybersecurity.

First, the government, through public attestations and its own security practices and procurement efforts, can help by recognizing IT products engineered for security. For example, the late Commerce Secretary, Malcolm Baldrige, was honored by having a quality award named after him and bestowed upon businesses that demonstrate outstanding quality in certain areas. We understand that the Department of Homeland Security is considering a similar award for high quality security solutions. We think this is a good idea and we are ready to support the government as it develops and implements this visible incentive.

Likewise, the government can lead by example by securing its own systems through the use of reasonable security practices and buying products that are engineered for security. Where appropriate—such as for national security agencies and other agencies, issues, and services for which security is of the utmost importance—this should include purchasing products whose security has been evaluated and certified under the internationally-recognized (and U.S. supported) Common Criteria for Information Technology Security. Such efforts to procure only security-engineered products, and specifically such clear support for the Common Criteria, will help strengthen the government infrastructure. In doing so, the government also will help set a high standard for security—one that ultimately is necessary to enhance the protection of critical infrastructures.

Second, public research and development can play a vital role in advancing the IT industry's security efforts. Accordingly, we support additional federal funding for cybersecurity research and development (R&D), including university-driven research. The public sector should increase its support for basic research in technology and should maintain its traditional support for transferring the results of federally-funded R&D under permissive licenses to the private sector so that industry can further develop the technology and deploy it widely.

Third, Microsoft believes that greater cross-jurisdictional cooperation and capability among law enforcement is needed for investigating cyber-attacks. Cyber-attackers can easily transit any border, as demonstrated by the I LOVE YOU and Anna Kournikova viruses and the Solar Sunrise attacks, all of which were international in scope. Enhanced law enforcement cooperation across local, state and international borders, along with increased law enforcement capability internationally, is vital for law enforcement to prevent and investigate cyber attacks. We therefore support an international law enforcement framework that establishes minimum criminal liability and penalty rules for cyber crime so that cyber-attackers cannot escape punishment for cyber attacks against the U.S. by seeking refuge outside of our borders.

Fourth, government has a critical role to play in facilitating information sharing. Government sharing its own information with industry is essential both to protect critical infrastructures and to build value in an information sharing network. In short, the government must be a provider as well as a consumer of valuable threat information.

Finally, government must recognize that even with the creation of the Department of Homeland Security and the new National Cyber Security Division (NCSD)—both of which Microsoft supported—cybersecurity remains an interagency problem. Accordingly, one of the key roles for the new Department, and specifically for NCSD, will be building incentives for effective government action, helping other government agencies develop new business processes that support homeland security, and reducing government stovepipes. Without a multidisciplinary effort by both government and industry, we will not succeed.

#### **Conclusion**

Microsoft is committed to strengthening the security of our products and services and is equally committed to working with governments and our industry peers on security issues, whether by offering our views on proposed regulatory and policy measures or participating in joint public/private security initiatives. In the end, a coordinated response to cybersecurity risks—one that is based on dialogue and cooperation between the public and private sectors—offers the greatest hope for promoting security and fostering the growth of a vibrant online economy.

Mr. THORNBERRY. Thank you.

We will now turn to our next witness, which is—who has already been partially introduced, Whitfield Diffie is vice president and fellow at Sun Microsystems, and has been one of, if not the key leader

in public key cryptography. And thank you for being here. You are recognized for five minutes.

**STATEMENT OF MR. WHITFIELD DIFFIE, CHIEF SECURITY OFFICER, SUN MICROSYSTEMS, INC.**

Mr. DIFFIE. Well thank you very much.

When people look back on this era we are in, the end of the twentieth century, the beginning of the twenty-first, I think what is going to be remembered is the era of a transition from a physical society to a virtual society, an information society, an electronic society. And things that we now regard as fairly arcane security mechanisms will come to be seen as fundamental social mechanisms in the same way that interpersonal recognition, which is a security mechanism, is perhaps the most fundamental mechanism of society.

Now, information security at this point is in my view 100 years old. There is a lot of prehistory, a lot of cryptography in the Renaissance and things like that. But the critical thing was the introduction of radio, because radio was the communications medium so valuable that nobody could afford to ignore it. And yet it was a medium in which all of the traditional security measures typified by the diplomatic pouch had no applicability at all. And consequently, cryptography was the only mechanism available to protect radio.

Now there are some other more technical ones, but cryptography is the most general one. And that swamped the code clerks.

First World War, they were working with techniques intended to encrypt a small volume of messages that were going to go into other protective channels. Suddenly they had to encrypt a vast fraction of what was communicated by radio. And this started a race to automation and a race to develop good cryptography that dominated information security for most of the twentieth century. I am pleased to say that I think that as a practical matter, we have largely solved that kind of problem. And I will just list one example of something that happened within the past few months.

Within the past 4 years or so, the U.S. adopted a new national cryptographic standard. It is called the Advanced Encryption Standard. And it was actually formally adopted the 26th of November, 2001. Unlike its predecessor, the data encryption standard, it was designed to be as secure as anybody could want. And that fact has been recognized this spring in the issuance of CNSS-15, policy memorandum from the Committee For National Security Systems, recognizing the AES is adequate to be used for the protection of classified national security data.

Now, there is still a long way to go. Even in that direction we are a long way from having the first piece of comsec equipment that uses AES. But this is a crucial milestone.

Later in the 20th century, communications security, cryptography centered security was joined by computer security. And in the first generation of this in the 1970s and 1980s, the envision was what was then called timesharing, lots of processes running on the same computer. That program was not entirely successful, although I am pleased to say that one of its best products is one of ours: Sun's trusted Solaris system is used widely throughout the federal government for high security applications.

But what happens if a secure computing, more than if the problem was solved, was that the problem changed?

And it became a problem of network security, and we went into—curiously, one of the greatest developments in security is something Sun not originated but certain pioneered, which is client-server computing: dividing functionality out among the computers of a network so that one appeals to another for services.

We introduced the Java programming language—a different style of writing programs with security very high among its qualifications.

Cryptography has become much more widely available and much better developed than it was back in the first period of computer security.

And the cost of hardware has fallen so that we can support computer security better with dedicated hardware.

In short, we have a whole new ball game. It also happens we have a whole new challenge.

Today when we say, as say a lot at Sun, The network is the computer, we are not saying a shadow of what we will be saying when we say that five to 10 years from now.

We are entering an era—the current buzzword is “Web services.” I don’t know if the buzzword will persist, but the concept will endure.

Computers communicating with computers and subcontracting work to them. You need data mining done? You need a movie rendered? You go out and you look at yellow pages, you find a computer, a resource that has the equipment to do this, and you get it done, they return their bill.

Suddenly we face a new set of security requirements and these are characterized by negotiation—one computer has to agree with the other what is going to be done; and by configuration control—a computer has to demonstrate to the other that it is capable of doing these things.

So we are in the infancy of a computer-mediated society and economy. And one of the critical things we know: We have to be careful. The decisions we make in security today are going to influence the structure of society all through the 21st century.

So we need both not to rush into regulation, particularly not to respond to disasters by sudden patch-up regulations, but to exercise foresight in this area to devote efforts to studying this area and to plan well for the security measures we need.

Very often the short sight of individual users drives security policy. They prefer what appears to be convenience in applications over a sound structure that gives them secure operation because they don’t anticipate the inconvenience of being broken into and having lots of down time. I think that government will have a big but what must be a very carefully considered role to play in this.

Security is going to be far more than just technology. It is going to influence law, it is going to influence business. The example I gave in my written testimony is: You capture the current contracting and subcontracting mechanism in things that happen in fractions of a second between computers. What are you going to do about adjudication? Nothing we have at the moment speaks to the

time scale and complexity of operation—of business operations—that is approaching.

I would like to close with one concrete suggestion, prefaced with some very important thanks. There was a proposal within the past year ago to move the computer security division of NIST into the new homeland security department. And we at Sun and many in industry thought that this was ill-considered because that division had learned over its 15 years of operation after the Computer Security Act of 1986 to work with industry, to field standards that industry actually accepted and used.

And we feared that the move into a department with a more military and more classified and more closed style would lead to standards that were not so enthusiastically received by industry.

So I would like particularly to thank representatives Boehlert, Goodlatte and Lofgren for their support in this matter.

But I think the computer security division at NIST needs much more support and has now a vital role to play. My colleague spoke about the importance of common-criteria certification for security processes. And that is a very valuable mechanism; it is very much in need of improvement.

The set of classifications within that system are complicated, hard for users to understand, hard for them to know the difference between something certified at EAL-2 and EAL-4. It needs to be simplified; evaluation needs to be improved and speeded up, but probably most important—something that the government is best placed to do—is that a validation mechanism for these ratings needs to be put in place, something that follows this history of evaluated products, determines whether they are really functioning securely, and is able to speed back the record of break-ins or attempted break-ins to these products in order to improve the evaluation products and guarantee that when we have security certification it really means the things are secure.

Thank you very much.

[The statement of Mr. Diffie follows:]

PREPARED STATEMENT OF MR. WHITFIELD DIFFIE, CHIEF SECURITY  
OFFICER SUN MICROSYSTEMS, INC.

When historians write the history of the late 20th century and the early 21st, they are likely to see it as the period when the world moved from the physical to the virtual. When face to face meetings, written letters, and visits to showrooms were progressively replaced by phone calls, e-mail, and web browsing. As information, and with it human culture, come to travel more and more in a digitized, computer-mediated world, the computer and communications infrastructure must be expanded to provide the fundamental mechanisms needed to support the totality of human culture. One of these, widely recognized but little understood, is security.

Information security: essentially, the protection of information in electronic media, is about a century old. The field has a long prehistory. Information has been protected on paper and in crude telecommunication channels, like signal fires, for millenia but information security as we know it today dates from the development of radio and from the use of radio in WWI.

The first major problem in information security was cryptography. Despite cryptography's romantic aura and long history, prior to radio, cryptography was always a secondary security measure. A dispatch on paper might be enciphered but its primary protection lay not in the encryption but in the careful handling of the diplomatic bag. Although telegraph messages were frequently sent in code, the customers were relying more on the integrity of the telegraph companies than on the codes for security.

The use of radio, particularly military radio in wartime, was different. Radio was so valuable that no one dared forgo its use. Prior to radio, Britain's First Sea Lord,

who commanded the largest navy in the world had only a vague idea of where his ships were. He might dispatch a flotilla on a mission and not hear anything about their progress for weeks or months. Within a few years of the introduction of radio, the First Sea Lord could expect to reach any ship in the fleet within hours. Today, of course, with the exception of submarines, this process is virtually instant, like making any other phone call.

The problem with radio from a security viewpoint is that everyone can listen to the radio and often the people you don't want listening get better reception than the ones you do. This promoted cryptography from a secondary security measure to a primary one. It was the only security measure of any use in protecting radio transmissions and it is still the primary one. The result was to swamp the code clerks, whose hand techniques were designed to add extra protection to a small fraction of military traffic, not provide the primary protection to most of it.

The result was the race to automate cryptography, and the resultant race to automate cryptanalysis, that dominated cryptography throughout the 20th century. For half a century, military cryptography was dominated by rotor machines: electromechanical devices that embodied cipher alphabets in rotating wheels and automated the polyalphabetic ciphers that had been known since Renaissance Italy but had been too prone to errors to see extensive use. Mechanization reduced the errors, increased the speed, and allowed much more thorough protection than could be achieved by hand.

In the 1930s, a new kind of rotor machine was developed in the US, one in which the wheels, of one rotor machine were moved by the actions of another rotor machine. This machine, called Sigaba, was the most secure cryptosystem of its era and it appears that no Sigaba traffic was read in the WWII period.

By the time of WWII, the US had secure cryptographic systems for protecting ten-character-per-second telegraph traffic but little ability to protect voice or other broader-band signals. The first secure telephone was developed during the war. The system, called Sigsaly, provided very secure, surprisingly comprehensible voice communications with one severe drawback: the system occupied thirty-racks of equipment, weighed as many tons, and cost millions. At first, the only customers who could "afford" Sigsaly were Roosevelt and Churchill. Even though, Sigsaly's were later provided to major military commands, there were never more than a dozen of them. However limited in deployment, Sigsaly was proof of concept for secure voice and the need to develop higher speed cryptosystems dominated cryptographic development for decades.

Although, like all important subjects, cryptography is still beset with profound unsolved problems, it is no longer the limiting resource in secure communication that it was for most of the 20th century. Good cryptographic systems are now available and the mathematical foundations on which they rest are widely understood.

The new status of cryptography is exemplified by the US Advanced Encryption Standard (Federal Information Processing Standard 197). AES is the successor to the US Data Encryption Standard (FIPS-46) which was adopted in 1977. At that time, the National Security Agency, recognized the need for a cryptographic system to protect government information outside the national-security sphere. Because such a system could not achieve its objectives without being made public, NSA worried that it would also be used by the enemies of the United States. The result was a compromise, a system that NSA considered strong enough for its intended application but weak enough that it would not present an insurmountable obstacle if NSA encountered a DES cryptogram that it felt sufficiently motivated to read. The development process, although formally open, was in fact closely held and the compromise became the subject of a long-running controversy.

When the DES came to the end of its useful lifetime in the late 1990s, the National Institute of Standards and Technology set out to replace it. This time the process was entirely different. After a public process of developing the requirements for the new algorithm, a solicitation drew fifteen candidates from around the world. The candidates were studied over a period of two years in a process that involved three public conferences. Five finalists were selected from the fifteen and then one winner was selected from the finalists. On the 26th of November 2001, an algorithm designed in Belgium was selected as the national standard of the United States.

To those who had watched the evolution of US cryptographic policy over the previous three decades, the AES seemed miraculous but an even more surprising turn occurred this spring, which was publicly announced in June. The Committee on National Security Systems of the Department of Defense issued Policy Directive 15, which authorized the use of AES (in approved implementations) for all levels of classified national security information. It will be years before we are applying COTS infosec technology to the majority of our national security systems but we have just passed a essential way point on that road.

Although, unification of other aspects of cryptography have not reached the same level of standardization, key-management techniques based on the first generation of public-key cryptographic systems is in use for both government and private sector security. Second generation key-management techniques based on elliptic curve cryptosystems promises a greater degree of unification within the decade.

In the latter half of the 20th century, cryptography was joined by another information security problem: secure computing. With the development of computers capable of running more than one program at a time, came the problem of running two different programs with different security levels or different owners and preventing them from interfering with each other. In the 1970s and 1980s there was great optimism about the prospects of developing a multi-level secure operating system.

This program called for extensive system specifications and formal verification that the systems met their specifications. This proved expensive and fewer systems emerged than had been expected. Among the successes is Sun's Trusted Solaris, a high-security operating system that is widely used in DoD and the Intelligence Community. In a reflection of the rising importance of security, the enhanced-security features of Trusted Solaris are being steadily integrated into the main-stream Solaris product and the two systems will be merged in the next major release.

Despite such isolated successes as Trusted Solaris, the problem of secure computing has been transformed more than solved. In the 1970s an organization of moderate size, such as Rand or the MIT Lincoln Laboratory would have a small number of big computers, perhaps only one. Every program that was run would have to be run on the one machine. If it was so sensitive that it could not be run in the presence of other programs, for fear that they might be spying on it, it would have to pay the high price of having the machine to itself.

As the seventies flowed into the eighties, two factors came together to change this. Computers got cheaper and became available at a variety of prices and a variety of levels of performance. Equally important, the ARPAnet, ancestor of the Internet, became available. This meant that a sensitive project no longer had to make arrangements for using a shared computer. It could purchase its own computer, appropriate to its needs an budget, put the computer in a room, and lock the door. Its communications with the outside world, if it needed any, could be handled through network channels more easily controlled than the communication paths internal to an operating system.

Client-server computing, the concept on which Sun was built, although rarely thought of as a security mechanism, has made a major contribution to security. In the network environment, a sensitive database can be isolated on a machine by itself, communicating with the rest of the world through a network connection. Enforcing the databases' access policies against users of other machines on a network is far easier than enforcing them against other users on the same machine.

Another key success in computer security came with the Java language. In the 1970s, DoD aspired to purchase "untrusted" applications, such as compilers and run them on classified data, in this case secret programs. Untrusted in this case means "uncleared." The programs in question came from reputable software manufacturers but from manufacturers who did not have DoD facility clearances or cleared workforces. In the 1990s, this objective was magnified several fold. With the rise of the Internet, it became valuable for client computers to import applet programs in real time from servers. As the cost of putting up a server is small, the applets no longer could be counted on to come from reputable computer manufacturers. "Untrusted" had reached a new level; a workstation needed the ability to run programs about which it knew nothing and get useful work out of them, without exposing itself to excessive risk. The Java solution is to write the programs in a portable language which is structured to allow the client machine to verify the structure of the incoming program before executing it.

Given the substantial effort that has been devoted to computer security over the past thirty years, the mixed results of that effort, and the fact that the need for security is steadily increasing, it is reasonable to ask what the prospects are today for major improvement. If one answers, as I would, that the prospects are quite bright, one must also answer the question "Why?"

As described above, the answer is that in large part, we are facing a new problem. The computer security problem seen in the 1970s has changed into a network security problem of the 21st century. Some problems have been solved, some problems remain, and many new problems have appeared. Equally important is the fact that new tools have become available. In the 1970s, cryptography was primitive by comparison with its development today. Two aspects of cryptography especially crucial to computer security, public key cryptography and hashing functions were in their infancy. Equally important, the National Security Agency, whose monopoly of cryp-

tographic erudition was far greater then than now, was the major backer of secure computing research but discouraged the application of much cryptographic techniques to the problem in unclassified research. The final piece of the puzzle is the ever-decreasing cost of computing. It is now feasible to dedicate computing capacity to security in a way that was not feasible even a decade ago.

An early example of a hardware-based approach to security problems is the domaining system of Sun's E12K and E15K servers. These servers can assign processors to processes and confine the resources available to those processes within a hardware-enforced domain. The effect is to combine much of the security advantage of running the process on an isolated computer with the advantage in cost and flexibility of running it on a shared computer.

It is a fair summation of our present position in information security that we have an excellent toolkit in the cryptographic area and a moderately good one in the computer security area. Having good toolkits is not the same as having good security, however; if it were, the security of the cyberinfrastructure would be far better than it is. Much of what needs to be done can be characterized as routine. New code needs to be written with greater care than has often been customary, old code needs to be repaired, and the security mechanisms that we know how to build—keying infrastructures, for example—need to be built, shaken down, and brought to a level of operational quality that allows us to depend on them. Other challenges loom on the horizon, however.

For as long as I have known the company, Sun has had the slogan: “The Network is the Computer.” and every year the slogan becomes truer. For years, it has been difficult for me to detect whether files I was using were on my own desktop or stored on a server some distance away. More recently, it has become possible to call on specialized computing and storage processes outside my own machine. These more recent techniques go under the name “Web Services.” At present most uses of web services involve interaction of a program currently being used by a human being—most often a browser—with a remote website supplying a service. In the near future—five or ten years at the most—this will evolve into a primarily computer to computer activity.

Today, the activities of both the public and the private sectors consists largely of business to business contracting and subcontracting processes. Some of these require great imagination and will for the indefinite future be performed by humans; others are routine and will be automated at a steady rate. Computers needing services will consult “yellow pages” directories of available services; choose providers according to price and capability; send out work orders; receive their results; and pay their bills.

Two sorts of web-based businesses are easy to foresee. The first are specialized businesses; businesses that offer a specific sort of service. They may have proprietary algorithms for such computationally intensive activities as graphic rendering or datamining; they may have access to specialized data such as the results of physical, biological, or social studies; they may have vast amounts of computing power. At present, Google provides an example of all three. It possesses vast amounts of computing power that it uses to build specialized databases, available to no one else, and it delivers information to its customers using specialized algorithms for both building and searching the databases.

A second kind of business that is in its infancy is more general in character: utility computing. As a business, utility computing is rather like property rental. Many companies, rather than owning property, rent their offices and often subcontract to their landlords the provision of furniture, food, environmental controls, etc. As utility computing matures, a startup—based perhaps on development of a new datamining algorithm—will no longer need to raise sufficient capital to have the powerful computer required to do production runs for its customers. It can wait for work to come in, then turn around and lease computing capacity from a “computer cycle provider.”

What sort of security measures will be required in this environment? They will parallel those of the current contractual mechanisms, particularly those employed for government contracts. When a system integrator contractor subcontracts the fabrication of a part for a military aircraft to a machining business, it is trusting not only that the work will be done correctly but that the plans for the part will be returned and that the subcontractor will not make extra copies for competitors. In choosing its subcontractor, the system integrator will seek a provider with a suitable facility clearance. Contracting on this scale is generally for work lasting from days to years and often reflects long-standing business relationships.

The computers will do it all faster. It is hard to predict exactly how far in the future this vision is but at some point, contracts for specialized data processing are likely to be negotiated and fulfilled in seconds.

The two problems that will be at the forefront of security research and development over the next decade are negotiation and configuration control. They will parallel existing business functions but they will take place at much higher speed and without moment-to-moment human oversight. The circumstances will incorporate many mechanisms now in use such as reputation assessment (clearance, Better Business Bureau membership) but in a far less forgiving environment. When contracting goes badly at present, problems are generally referred to the courts. When contracting goes badly on the scale of seconds, what mechanism will step into the breach?

As we move our economy and society further and further into computer mediated telecommunication channels, the role of cybersecurity in homeland security will grow steadily. There will not be general agreement on the proper course of action. Our decisions will advantage some legitimate parties and disadvantage others. The solutions to the problems that arise will thus be as much legal and political as technical and will tax both our resources and our imaginations.

Mr. THORNBERRY. Thank you, sir. We will now turn to Dr. Craig Lowery, who is chief security architect and a software architect and strategist at Dell Computers.

Welcome, sir, you are recognized.

**STATEMENT OF DR. JAMES CRAIG LOWERY, CHIEF SECURITY ARCHITECT/SOFTWARE ARCHITECT AND STRATEGIST, DELL COMPUTER CORPORATION**

Dr. LOWERY. Thank you Chairman Thornberry, Ranking Member Lofgren, members of the subcommittee. My name is Craig Lowery, software architect and strategist for Dell.

We are very pleased to be here this morning, and we would like to wholeheartedly concur with your opening themes of partnership and consensus, because Dell believes that that is the best way to go about achieving more secure systems for everyone. Since everyone is using these systems, we all play a role.

We see a universe of technology which has vendors and customers that are working in partnership together. It is not reasonable to think that one party or the other has a complete key to solving the security puzzle.

Vendors bring products to market, and they must make reasonable allowances for security as part of the design of those products. And customers have a responsibility, too, in the way that they deploy those products.

It is possible to create a product that is "secure," when it is shipped as a single component, but when it is placed into an aggregate configuration it could very well be part of an insecure infrastructure that is created.

So it is not a one-sided approach that should be considered to solving the security puzzle. It has to be partnership-and consensus-driven. One of the things that is defining about Dell as a company is its direct business model, which you may have heard about.

If you haven't, I will give you just a little bit of a glimpse into it, because it very much influences how we are approaching this problem, among others.

The direct business model means that Dell believes that having direct relationships with our customers is the best way to go about delivering solutions to them, because we can hear directly from them the problems that they are having, they are trying to solve, the solutions that they need.

One way to arrive at consensus of customer input, customer feedback, is through standards. We are a very standards-oriented com-

pany. We prefer to deliver standards-based solutions, because we believe that that is, first of all, something that has gone through a consensus process, either formal or sometimes more informal, through user groups.

We also see that that consensus process develops a standard which everyone understands, there are no surprises, and can be delivered to, we can deliver products to that. That is very much in line with our direct business model.

One of the concrete examples that I have for you this morning of this strategy at work is a new offering from Dell which is based on work that is been done by a group called the Center for Internet Security, or the CIS.

The Center for Internet Security is a group of users across sectors of industry, government, education, finance and health care, who have gotten together their security experts and have pooled their knowledge of experience and best practices, the best way to go about securing things.

And the product of this group is a set of things called benchmarks. These benchmarks are settings for pieces of software, such as operating systems, which the users that are members of the CIS agree are the best settings, according to their research and their work.

At the request of our government customers, we have taken those settings for Microsoft Windows 2000 and we are now making those settings available direct from our factory, pre-installed, on certain products, specifically our Optiplex, our Latitude notebooks and our Precision Workstations.

This is the direct result of our philosophy and the work of the consensus mechanism in the industry to bring about immediate changes into the security landscape at this time.

We certainly see that security is a moving target, and that as things progress these improvements will appear not as a change to settings that we have to make, but that are going to be built directly into software products, and we see that already happening at the source.

We are also working in other areas to deliver more secure solutions to our customers at their request, things like smart cards, which are a form of authentication that has been requested by customers.

We now have smart card readers built into our D series Latitude notebook computers, and also we have keyboards for our systems which read smart cards.

We have biometric technology, which we have been evaluating, and we have decided that some of those solutions meet our requirements and those of our customers, and we are now making those things available through our Software and Peripherals Department.

Standard physical locks for chassis and racks and things like that are always something that we are attending to and making sure are securing the physical hardware, and new types of products, for example, such as fire walls, which we are making available through Dell to our customers so that they are able to get their security solutions, or most of their computer solutions, directly from us.

So in summary, we do believe that security is best achieved in partnership and consensus, things we are very happy to hear that are being expressed here today.

Our direct model, we believe, puts us in a position to really make use of standards and to help disseminate that kind of information. The CIS offering is a concrete example of that in action.

We continue to evaluate best-of-breed solutions in the security space and bring them to market as our customers request them.

Thank you for your time.

[The statement of Dr. Lowery follows:]

PREPARED STATEMENT OF DR. JAMES CRAIG LOWERY, PH.D.

Chairman Thornberry, Ranking Member Lofgren, and Members of the Subcommittee, thank you for the opportunity to discuss Dell's perspective on cybersecurity and the role of technology, specifically hardware and software security products. My name is Craig Lowery and I am the chief security architect in the Dell Product Group.

Headquartered in Round Rock, Texas, a suburb of Austin, Dell was founded in 1984 on a simple concept: that by selling computer systems directly to customers, Dell could best understand their needs and efficiently provide the most effective computing solutions to meet those needs. Today, Dell is the world's leading computer systems company. The company employs approximately 40,000 team members around the globe. We design, build and customize products and services to satisfy a range of customer requirements from the desktop notebook, server, storage and professional services needs of the federal government agencies, to those of the largest global corporations, and to those of consumers at home.

To fully appreciate Dell's security strategy, one must understand Dell's direct business model. We believe that the best customer solutions are most efficiently derived through direct relationships with our customers and suppliers. Our build-to-order system allows customers to order computers tailored to their needs, manufactured specifically for and delivered directly to them. We believe that customers receive the best value from products built with standard technologies; to that end, we seek to foster standards throughout the industry to reduce cost and increase customer flexibility and choice. As I will explain, each of these facets of the direct model plays a key role in how Dell is approaching computer system security.

Cybersecurity has become increasingly important for our industry due to the need to provide products to our customers to better protect their IT systems from cyber attacks and viruses. Until recently, most company security solutions have been proprietary and customized to fit their specific needs. As the need for IT security has grown from supporting specific applications to that of protecting critical IT infrastructure, our industry, including Dell, has pushed for standardization to make security more affordable and widely available.

As a technology vendor, Dell is committed to delivering value through reducing the costs of acquisition, deployment, interoperation and maintenance of our products, including our security products. Dell believes that these benefits are best achieved through the benefits of industry standard technologies. Specifically, Dell believes that standards in the security arena are driving and will continue to drive these technologies to levels of maturity that make them more transparent to the end-user and thus suitable for widespread adoption in the industry. As these technologies mature, Dell leverages the benefits of its direct model to bring these technologies to market quickly and affordably.

Securing information systems is only possible through partnership between vendors and customers. Security is a moving target, and the products and services addressing security needs necessarily evolve as the landscape changes. Vendors are responsible for bringing to market products that incorporate widely accepted security design goals. Customers are responsible for deploying the products in a manner consistent with effective security best practices. Vendors must be open to customer feedback to understand their security concerns, and customers must be diligent to provide that input.

Dell is placing more and more emphasis on security as a chief design consideration in all of our products. Certainly as a hardware vendor, we are acutely aware of the need for physical security through mechanisms such as locks and detection devices. Our efforts to deliver more secure products extend beyond hardware. Since we custom-build the systems we ship, including factory installing operating systems and applications, we have the opportunity to continually improve upon the software

configurations we offer to customers. We work closely with software providers during their design and implementation phases. We are able to identify and integrate tested security components into our factory-installed software so that customers can enjoy the benefit of best solutions “out-of-the-box.” Pre-installed virus protection is one example.

An important security benefit of our build-to-order system is that it reduces the time between when we make changes to our products in the factory, and the time a customer receives the product. Therefore, if we improve the security of a product, our system helps to minimize the lag time in getting it to the customer since there is no inventory that must first be moved in the distribution channel.

Another example of creating an even more secure software configuration is a new Dell offering available through our custom factory integration unit. Dell is beginning to offer desktop systems installed with Microsoft Windows 2000 pre-set to the Center for Internet Security’s Level I benchmark. This is a separate offering from our “normal” Windows 2000 installation, which continues to be available.

The CIS Level I benchmark is a consensus standard which the CIS considers the best and least restrictive security settings for Windows 2000. These settings were developed with input from government agencies, business, universities, and individual security experts. In providing the factory installed benchmark systems, Dell is responding to customer demand for a hardened operating system direct from the factory. Although it is designed for our public segment customers such as federal, state and local governments, this product can benefit any organization wishing to receive a certain level of security with a system directly from Dell.

System BIOS passwords and hard-drive passwords continue to play an important role in security. For even more robust forms of authentication and access control, Dell now offers integrated smart card readers in our Latitude D-family notebooks as a standard feature, and in our smart card reader keyboard for desktops. In addition, Dell offers biometric authentication solutions in the form of add-on peripheral devices. Dell is actively involved in new developments in wireless security standards such as Wi-Fi Protected Access, and the emerging 802.11i standard.

Through our software and peripherals department, Dell is able to provide customers with thirdparty solutions that meet their demanding standards, such as wireless products, firewalls, and security software.

Again, security requires cooperation between vendor and customer. At Dell, we know our customers face many challenges when it comes to successfully deploying an IT infrastructure that is secure, usable, and manageable. We provide deployment and management assistance to our customers in several forms to help them in these efforts.

In addition to telephone support, Dell provides access to our technical support web site. Premium technical support is available to customers requiring even faster response. Our engineers develop white papers and journal articles targeting many content areas, including computer system security. These articles are also freely downloadable from our web site at [dell.com/powersolutions](http://dell.com/powersolutions). We are actively engaged with security organizations such as the SANS Institute, the CERT Coordination Center, the Center for Internet Security, and the Free Standards Group.

Dell also makes available pre-packaged and customized services, helping to ensure consistent, repeatable processes for our customers. Dell’s service offerings include everything from onetime services to deploy and configure, to fully managed solutions where we take on the day-to-day tasks of running your IT infrastructure. Security is one of many aspects we consider in providing these services to our customers.

Dell is a security-aware and privacy-aware company. We know that security is of increasing importance to our customers, and we are striving to deliver more secure products and services, as well as those that are security-specific, as they become available. We deliver security solutions in a way that is consistent with Dell’s model: quality, low cost, easily integrated standards-based solutions that meet our customer requirements, delivered directly to them. We look forward to working with this Subcommittee as it considers ways to improve cybersecurity.

Thank you again for inviting me to participate in today’s hearing and for seeking Dell’s perspective on cybersecurity. I would be happy to answer any questions.

Mr. THORNBERRY. Thank you, sir.

As my colleagues can tell, we have roughly divided up the witnesses into two groups. We have heard from three witnesses that are roughly in the field of products, and now we are about to turn to three that are roughly in the field of services although with these companies, clear lines are difficult to draw.

We will now turn to Jay Adelson, who is a founder and chief technology officer of Equinix, which is the largest independent, or neutral, provider of interconnection and data center services in the world.

Welcome, sir. You are recognized for five minutes.

**STATEMENT OF MR. JAY ADELSON, CTO & FOUNDER, EQUINIX, INC.**

Mr. ADELSON. Thank you. Chairman Thornberry, Congresswoman Lofgren, distinguished members of the committee, I sincerely appreciate having the opportunity to be here today as a representative from Internet industry, and more specifically, the perspective of critical Internet infrastructure, the Internet itself, network access points, or commonly known as Internet exchange points.

As you said, my name is Jay Adelson. I am the founder and chief technology officer of Equinix. And the reason Equinix has a unique perspective on the issue of Internet security is, as you said, we are the largest neutral provider of interconnection. Equinix's facilities, therefore, serve as the meeting places for all the various elements of Internet, ranging from enterprise users, large Internet Web sites, network providers, telephone carriers, cable companies and subscriber services.

Much of the Internet industry knows us as an exchange point or NAP where most of the Internet traffic in the United States, or significant portions, converge as they pass from one network, such as AT&T, to another, such as AOL, as well as the place where important sites, such as Google, Yahoo, Paypal, IBM customers and others place their critical infrastructure.

A good analogy for an exchange point is that we function as an international airport for Internet networks and services. And our airlines are networks and our travelers are data bits and bytes. There are 100 exchange points in the world bearing services and levels of security though, in common, they all facilitate this exchange of traffic.

While my distinguished panel members are part of well known, large vendors and network service providers, the chances are, while you may not have been exposed to Equinix in the past, you stand to receive e-mail that traverse our exchange points and surf Web sites housed in our facilities. The very fact that Equinix is a physical part of the Internet infrastructure, where such a large percentage of the Internet itself, happens is not as well known. It illustrates the fact that the Internet itself is a massive structure interconnecting independent entities very difficult to accurately measure, monitor, and international in scope.

Equinix, like international airports, focuses heavily on the physical security of our data centers. And we have instituted check points, audit trails, people traps, steel cages, layers of biometric security, et cetera, and very strong security operations procedures. Our customers demanded these in the late 1990s when we built them. And we based the security design and requirements from our financial service customers and recognize that there was no physical security standard on which to build and base our new design.

We were not able to find any of these reference standards to the level of security operation procedure we felt, and our customers felt, were appropriate for such an important hub as Internet traffic. It didn't exist. So, therefore, we made a conscious decision, as part of our business plan, to be the most physically secure exchange point in the United States.

But this model is fairly unique in that market forces allowed us to develop this new approach to providing heightened physical security.

A balance must be achieved between network service providers, hardware vendors and their users. Ultimately, users must bear, as my colleagues suggested, the largest responsibility for protecting their assets. Network service providers and software and hardware vendors supporting the Internet industry can only empower the Internet users with systems and services that enabled secured use of the Internet.

There are strong economic limitations to the scope of physical and logical protection network service providers can reasonably implement. But at a minimum, a baseline standard of configuration and administration can be met.

The cyber and physical security best practice, developed by the Network Reliability and Interoperability Committee, are a good example of how infrastructure operators are able to provide baselines for all network operators to follow. These range from information about network configuration to background checks for employees in critical facilities. And as a nation, we must continue to advance research and development to increase the embedded security level as well as support these standards at the network level and with edge users.

There are a surprisingly high number of autonomous networks and systems that affect the health of the Internet. A common misunderstanding is that only a few very large networks, known as backbones, create the largest impact.

As incidents of the past have taught us, there are many more players, enterprises, domain name service providers, foreign networks and small regional networks that can impact network stability and security.

These entities are scattered all over the world, their security policies and procedures are as diverse as the networks and services that they operate.

While information sharing with the federal government is a newer concept in the Internet arena, information sharing is fairly robust within the Internet technical community, and it has to be. We are all customers and providers to one another, and a major failure on the Internet impacts all infrastructure operators at the bottom line.

We communicate with our account reps, our technical help desk, our emergency contacts, to restore services as quickly as possible. It is not clear, however, how to integrate the federal government into the commercial information-sharing exchange.

The government has an opportunity to act as a means to spread the word during a crisis, and tools such as the Cyber-Warning Information Network are a good start, although the original intent of these systems must not be diluted.

Opening the communication channels is critical when every second counts, but choosing what data is appropriate through ISAC-to-ISAC communications, versus leaving it open, limits their effectiveness.

The federal government must do more to expand information-sharing with infrastructure owners, and establishing the National Cyber-Security Directorate at the Department of Homeland Security is a good first step.

In the event of a cyber-crisis, it is important for the Department of Homeland Security to understand that the infrastructure owners, the network operators in particular, are the first responders.

Speed is of the essence in responding effectively to these types of crises, and therefore adding communications steps and information management runs the risk of slowing down the response.

For infrastructure operators, the Internet is first and foremost a commercial enterprise, and thus restoration of service is critical in order to meet the service level agreements with customers, as well as to support the Internet commerce generally.

This must be recognized as processes are developed, and, as well, centralization of all this information will improve accuracy in communication. The methods of information distribution must be relatively instantaneous and flat in hierarchy.

In conclusion, Equinix strongly supports the work of the Department of Homeland Security in working to promote both physical and cyber-security for our nation's networks. And I very much appreciate the opportunity to testify here today, and would be happy to answer questions that the committee may have.

[The statement of Mr. Adelson follows:]

#### PREPARED STATEMENT OF MR. JAY ADELSON

Chairman Thornberry, Congresswoman Lofgren, distinguished members of the Committee; I sincerely appreciate having the opportunity to be here today as a representative from Internet industry, and more specifically, the perspective of critical infrastructure of the Internet itself, the Internet Exchanges, or Network Access Points (NAP).

My name is Jay Adelson, and I am the Founder and Chief Technology Officer of Equinix. The reason Equinix has a unique perspective on the issue of Internet security is that we are the largest independent, or "neutral," provider of interconnection and data center services in the world. Equinix's facilities serve as the meeting places for all the various elements of the Internet, ranging from enterprise users, large Internet web sites, and network providers such as telephone carriers, cable companies and subscriber services.

Much of the Internet industry knows us as a NAP operator, or Network Access Point, where most of the Internet traffic in the United States converges as it passes from one network, such as AT&T, to other large networks, such as UUNet or AOL, as well as the place where important web sites, such as Google, Yahoo!, PayPal, or IBM customers, place their critical infrastructure.

A very good analogy for a NAP operator is that we function as an international airport for Internet networks and services, though our airlines are networks, and our travelers are the data bits and bytes. There are over a hundred NAPs throughout the world, varying in services and levels of security, though in common they all facilitate the exchange of Internet traffic.

While my distinguished panel members are part of well known, large network service providers, chances are that while you may not have been exposed to Equinix, you have sent or received e-mails that have traversed our exchange points, and surfed websites housed in our facilities. The very fact that Equinix, as a physical part of the Internet infrastructure, where such a large percentage of the Internet passes, is not as well known, illustrates the fact that the Internet itself is a massive structure of interconnecting, independent entities, very difficult to accurately measure or monitor, and international in scope.

#### Role of Industry and Equinix In Securing Cyberspace

The Internet exists on multiple layers, both the physical and the logical. At the physical level, the industry has a long way to go to secure itself. While some infrastructure operators provide advanced cyber and physical security, some operators have not yet incorporated security into their basic business plan. This provides the Internet industry as whole with much room for improvement.

Equinix, like international airports, focuses heavily on the physical security of our datacenters, and have instituted checkpoints, audit trails, man traps, steel cages, five layers of biometric security, high-availability video, concrete embankments and strong security operations procedures. Our customers have demanded this physical security from our facilities. When we built them in the late nineties, we based the security design on the requirements from our financial services customers, and recognized that there was no physical security standard upon which to base our new design. We were not able to find any reference standard for the level of security operations procedure we felt, and our customers felt, was appropriate for such an important hub of Internet traffic. It simply didn't exist.

Equinix, therefore, made a conscious decision as a part of our business plan to be the most physically secure NAP operator in the United States. However, our model is fairly unique in that market forces allowed us to develop a new approach to providing heightened physical security for critical Internet assets. At this point, Equinix's customer base represents over 90% of the Internet routing table, as over 120 of the largest and most prolific Internet networks use our locations as their critical hubs.

Equinix, as a central exchange point between networks, will continue to do our part to physically secure the Internet assets. At the logical level, the implementation issues are international in scope, with literally thousands of independent players requiring education and motivation to adopt modern security practice.

#### Industry Responsibilities

A balance must be achieved between network service providers, hardware vendors, and their users. As secure as a network may be from compromise, or as many features that a hardware or software vendor places in their products, ultimately users must bear the largest responsibility for protecting their assets.

Network service providers, and software and hardware vendors supporting the Internet industry can only empower the Internet's users with services and systems that enable secured use of the Internet. There are strong economic limitations to the scope of physical and logical protections network service providers can reasonably implement, but at a minimum, a base-line standard of configuration and administration can be met.

The cyber and physical security best practices developed by the Network Reliability and Interoperability Committee (NRIC) are a good example of how infrastructure operators are able to provide baselines for all network operators to follow. These range from information about network configuration to background checks for employees in critical facilities. However, best practices are often difficult and costly for smaller networks, enterprises, universities, governments, or individuals to implement. As a nation we must continue to advance research and development to increase our imbedded security level, at the network level and with edge users.

#### Information Sharing

There is a surprisingly high number of autonomous networks and systems that affect the health of the Internet. A common misunderstanding is that only a few, very large networks, commonly known as backbones, create the largest impact. As incidents of the past have taught us, there are many more players, including enterprises, content providers, domain name server operators, foreign networks and small regional networks, that can have significant impact on network stability and security. Recent research Equinix conducted shows evidence of there being over 13,000 entities, not including network service providers, in the global Internet that manage their own multi-network connectivity, injecting their network information into the global Internet. These entities are scattered all over the world, and their security policies and procedures are as diverse as the networks and services they operate. While abuse from one of these entities can be mitigated through good security practice, a large number of them are as relevant in information sharing as the network operators themselves.

While information sharing with the federal government is a newer concept in the Internet arena, information sharing is fairly robust within the Internet technical community. It has to be—we are all customers and providers to one another, and a major failure on the Internet impacts all infrastructure operators at the bottom line. We communicate with our account representatives, with our technical help desks, with our emergency security contacts, to restore service as quickly as pos-

sible. What is not yet clear, however, is how to integrate the Federal government into the commercial information sharing exchange.

#### How the Federal Government Can Help with Information Sharing

The Federal Government has the opportunity to act as a means to spread the word during a crisis as a central moderator. Tools such as the Cyber Warning Information Network are a very good start, although the original intent of these systems to be a tool during a crisis for the Internet community must not be diluted. Opening the communication channels is critical when every second counts. Choosing what data is appropriate for ISAC to ISAC communications, versus leaving it open, limits their effectiveness.

The Federal government must do more to expand information sharing with Internet infrastructure owners. Establishing the National Cyber Security Directorate at the Department of Homeland Security is a good first step. However, for the Federal government to become a trusted partner for information sharing purposes, it will have to develop business plans and models to highlight how and where the government is best suited to assist the Internet infrastructure in protecting and restoring itself.

#### The Role of the Department of Homeland Security

The DHS has two unique and immediate functions that it should provide to infrastructure operators. First, DHS should provide a platform for information to be shared, amongst infrastructure sectors, and to the states. Second, DHS should be working in partnership within industry to promote the development of cyber security standards and baselines, to ensure a national approach to cyber-security. Clarifying the Federal government's role as the "Public" partner in our Public—Private Partnership, cited in the National Strategy, to Secure Cyberspace, will be a critical task for the new Cyber Security Directorate. A network operator, content provider, or NAP operator all have different roles to play in a crisis, and the value of the response will be contingent upon the DHS having a clear understanding of what data is appropriate for which group, and what action, if any, the government is capable of taking.

In the event of a cyber-crisis, it is important for the DHS to understand that the infrastructure owners, the network operators in particular, are the "first responders." Speed is of the essence in responding effectively in these types of crisis, and therefore adding communication steps and information management runs the risk of slowing down the response. For infrastructure operators, the Internet is first and foremost a commercial enterprise, and thus restoration of service is critical, in order to meet service level agreements with customers, as well as to support Internet commerce generally. As a result, crisis communications at the technical level between the largest infrastructure operators is generally very good. Trust and experience has played a large role in increasing the response capabilities of the largest infrastructure operators, and the government will have to develop trust and experience as it becomes a part of cyber-security. This must be recognized as processes are developed, as while centralization of the information will improve accuracy, the methods of information distribution must be relatively instantaneous and flat in hierarchy. Working with industry as the "first responder" will be an immediate challenge, and a new paradigm for DHS that requires dedicated effort.

In conclusion, Equinix strongly supports the work of the Department of Homeland Security in working to promote both physical and cyber-security for our nation's networks. I very much appreciate the opportunity to testify today, and would be happy to answer any questions that the Committee may have.

Mr. THORNBERRY. Thank you, sir, appreciate it. Frank Ianna has been with AT&T for more than 30 years, including most recently as president of AT&T network services.

Earlier this year he announced his intention to retire, but they can't let him go. And so we are glad you are here within us today, sir, and now you are recognized for five minutes.

#### **STATEMENT OF MR. FRANK IANNA, PRESIDENT, AT&T NETWORK SERVICES, AT&T CORPORATION**

Mr. IANNA. Chairman Thornberry, thank you very much, Congresswoman Lofgren and members of the subcommittee. Let me summarize my testimony with several points, and then recommendations under some of those points.

First, along the idea of cyber and physical security. Cyber-threats are particularly challenging to the service industry for four reasons.

First, attackers do not need a physical presence or a large investment in a physical presence to cause harm. They could do it remotely.

Point number two is that all vendors of products and services, hardware and software, whether they are switching elements or computing elements, have critical roles to play in enhancing the overall cyber-resiliency of mission-critical services.

And several recommendations can spring from this, such as software and equipment vendors and network operators and standards bodies should have products that have built-in baseline security features. With system administration, any interaction of these should be made simple.

Service providers and vendors should collaborate also to develop an overall security management system so that we could see very instantaneously the traffic anomalies happening on networks, then we could respond very quickly too.

And the government can stimulate development of more secure products by funding research and development of inter-operable software and hardware standards to provide network management described above.

The third point is that there is extensive interconnection, as some of my colleagues have mentioned, this is very nature of communications among telcom and IP providers and data network providers.

And each of these carriers are interconnected to form a service for a consumer or a business.

We must help each other. And we have to communicate with each other, our operations centers, on a continuous basis. A significant failure in one network can cause a significant failure in another network. And in many cases, the symptoms of a failure in one network actually show up first in the other network.

Carriers today do share network disruption information directly between their operation centers, ours, the global network operation center in Bedminster and all the other carriers that we interface with, and with the Telecom Information Sharing and Analysis Center, the Telecom ISAC, today.

For example, the slammer worm that we detected on January 25, 2003 was the fastest-spreading worm in history, but industry worked together with the Telecom ISAC and with government to share our mitigation plans, our strategies and our notification procedures.

Point number four, insider threats to our network should not be discounted. A malicious insider may easily circumvent cyber-security protections employed to discourage outside threats. So a recommendation here would be to have infrastructure providers and governments work together to develop a process to ensure that all employees and contractors with access to critical facilities undergo background checks, screening and National Crime Information Center reviews.

Now, the next point is talking about public and private partnerships. What we are saying here is that there is a good opportunity

to have a public/private partnership with the government. The telecom ISAC, for example, is a good example of this, it is the number one long-standing public/private partnership in telecom.

Point number six, is companies will only engage in sustained and meaningful information sharing when there is a compelling business case to do so and only in a trusted environment. And this is for two related reasons. The government should consider adopting the NCC funding model to enhance effectiveness of other ISACs where the government is actually funding some of the infrastructure for us to communicate amongst each other.

For example, the round-the-clock staffing is not borne exclusively by the private sector, it is borne by the government. And the government partners provide value back to the industry. Two examples here, the government should provide value to other ISACs in the form of useful and timely threat information, and supporting industry's response recovery efforts during the crisis.

The NRIC, as my colleague here mentioned, the National Reliability and Interoperability Council, which is really the sixth incarnation of that council created every 2 years, is a long-standing partnership that the FCC and the Telecom industry started in 1992.

The FCC—and point number seven—has wisely recognized that to be successful, the effort must be: number one, voluntary; number two, developed by industry experts; and number three, adaptable to different network providers to reflect differing architectures and approaches. What constitutes a network failure in a wire line voice network is very, very different than what constitutes a failure in an IP-provided network, for example.

Two final points here. Number one, information about physical locations and capabilities of network infrastructures must be carefully safeguarded. We have seen instances where much public information has been put out and there are lot of requests for information. We recommend here that particularly we work with the Department of Homeland Security and particularly the states.

We may not be only getting one request from the federal government, and we actually could be getting 50 requests from different states to provide very macro and very specific threat and vulnerability information. And we believe that the Department of Homeland Security should be the focal point for coordinating process amongst all federal agencies and states so that we ensure that the information is properly managed.

And then finally we should expand our public and private partnership. Private sector critical infrastructures providers must have the opportunity to provide input to portions of the new national emergency response plan that address how the private sector would respond in a national crisis. I would like to thank you for allowing me to make these comments, summarizing the positions that AT&T has from our experience in these industries. Thank you very much.

[The statement of Mr. Ianna follows:]

#### PREPARED STATEMENT OF MR. FRANK IANNA

Thank you for this opportunity to testify on behalf of AT&T regarding industry views on cyber security. My name is Frank Ianna, and I am the outgoing President of AT&T Network Services. My testimony will describe AT&T's views on several aspects of this very important issue.

AT&T is among the premier voice and data communications companies in the world, serving businesses, consumers, and government. The company runs one of the most sophisticated communications networks in the U.S., backed by the research and development capabilities of AT&T Labs. A leading supplier of data, Internet and managed services for the public and private sectors, AT&T offers outsourcing and consulting to large businesses and government. With approximately \$37 billion of revenue, AT&T has about 40 million residential customers and 4 million business customers who depend on AT&T for high-quality communications. As such, we have an overarching interest in preserving and promoting a safe, secure and robust infrastructure that will be a key enabler of economic growth and prosperity of the United States. We therefore very much appreciate the opportunity to offer these comments today.

#### **Cyber vs. Physical security:**

Sound security practices obviously must address both physical risks and cyber risks. Cyber security risk management is more focused on the “logical” or user’s view of the way data or systems are organized as compared to physical security risk management of our network which is topology/technology-focused. But cyber threats are particularly challenging for at least four key reasons. First, attackers do not need physical presence to do significant harm, and a cyber “saboteur” could launch attacks from anywhere. Nor does it take a large investment to launch a cyber attack, only a PC and access to the Internet.

Second, the availability and deployment of cyber security capabilities is not only a service provider issue, but requires the involvement of product developers, vendors, and end-users. Software code is becoming increasingly complex and the number of lines of code is multiplying at an incredible rate. Thus no single entity has complete control over the security of its product or service. The very structure of today’s hearing reflects that reality - that all vendors of products and services have critical roles to play in enhancing the overall cyber-resiliency of mission-critical services. Industry, standards bodies, software and equipment vendors, network operators, and end-users of all products and services that make up the Internet should ensure that these products have built-in baseline security features and that these features are appropriately configured and kept up-to-date. System administration of current cyber products is much too difficult. Vendors need to be encouraged to simplify their products and employers need to increase the level of expertise required to perform this vital task.

One specific area in which service providers and vendors could cooperate that would make a vast improvement in cyber-security is in the development of an overall security management system that would provide detailed traffic statistics to the Network Operations Centers of major IP backbone providers about the transmission of packets on our networks and detect and respond to anomalies, as we do today in our public switched telecommunications network.

Government can also play a key role in stimulating development and deployment of more secure products and services, not by trying to impose compliance at some arbitrary level, but by funding research and development of interoperable software and hardware standards to provide the network management that would enable network operators to detect and stop malicious attacks in the core network. Government can also create strong incentives for the deployment of these capabilities through its purchasing power as a user of more secure cyber capabilities.

Third, because there is extensive interconnection among telecommunications and IP networks, carriers must assist one another because a significant failure in one network can affect another network. In fact, telecommunications carriers today share network disruption information directly between Network Operations Centers, and with the sector Information Sharing and Analysis Center (ISAC). The Slammer worm, which was detected on January 25, 2003, was the fastest spreading worm in history. This worm affected more than 90 percent of vulnerable hosts within 10 minutes, far more quickly than Code Red of 2001. Industry participants worked together through the Telecom ISAC and with the government to share mitigation plans. The good news is that the Slammer worm had no payload; the bad news is that a similar worm could be launched with a malicious payload. We need to be better prepared by building more secure technology and employing better processes to support security controls for the entire network.

Lastly, though cyber threats can originate anywhere, the insider threat should not be discounted, because a malicious insider may easily circumvent cyber security protections that are deployed to discourage outside threats. To address this issue, providers of critical facilities must work with others in industry, and with government at all levels to develop and employ a standard process to ensure that all employees and contractors with access to critical facilities undergo appropriate background

checks, screening, and National Crime Information Center reviews. Government can play a key role by helping to develop the most efficient process, and by acting as a centralized resource to coordinate requests from industry for reviews. This is good and will help.

Now, having said that, I want to add that those service providers of critical infrastructure have had to solve the problem of access long before it became prominent following the events of September 11. Many people enter and leave critical infrastructure facilities every day. The location may be any location where multiple providers have placed facilities and equipment. These individuals may be communications technicians from different service providers who are maintaining equipment housed in the building. There are others who also may need to gain access to a building, such as power contractors, janitors, vending machine operators, copying machine technicians, etc. During the day, any number of non-communications-related individuals go in and out of telecom buildings. One solution that AT&T has implemented is to escort all non-badged individuals who need access to critical locations. AT&T has made strong security a top priority for many years, but because we are so extensively interconnected with other infrastructure operators, we must also closely cooperate with our peers, arguably to a greater extent than in any other infrastructure. Our industry has of necessity been a leader in the information sharing process long before the President's Commission on Critical Infrastructure Protection and PDD-63 recommended the formation of sector-specific, information sharing forums in May, 1998.

#### **Developing an effective "public-private partnership":**

As you know, most of the country's critical infrastructures are owned and operated by the private sector, thus the private sector must play a key role in safeguarding those infrastructures. With cyber security, the private sector has an even more important role, because the responsibility for implementing adequate security measures falls not only on core infrastructure providers like AT&T, but also on government and business enterprises that deploy and rely on cyber information systems to perform business-critical functions. For these reasons, much has been said about the need for an effective "public-private partnership" to share security-related information and to address security-related threats and vulnerabilities. These are laudable goals, and in fact, AT&T and other telecommunications companies have been working together to identify and address security risks, and to develop security-related best practices in partnership with government, for many years. Two of the most significant partnerships are noteworthy.

#### **The Telecom-ISAC**

Much of the benefit attributed to a partnership between government and industry involves the need to encourage robust, timely, two-way information sharing about threats, vulnerabilities, intrusions and anomalies. New protections provided in the recently enacted Homeland Security Act significantly reduce the possibility that sensitive information shared voluntarily for these purposes might be disclosed publicly. Nevertheless, companies will only engage in sustained and meaningful information sharing when there is a compelling business case for doing so, and only in a trusted environment. We at AT&T have a lot of experience in this area. Telecommunications carriers have shared information informally with the National Communications System (NCS) since 1984. In 1991, the National Security Information Exchange (NSIE) was established as a forum in which government and industry could share information in a confidential, trusted environment. Since March of 2000, the NCS's National Coordinating Center (NCC) has served as the Information Sharing and Analysis Center, or "ISAC" for Telecommunications. Telecom-ISAC participants, including industry and government representatives, gather and share information on threats, vulnerabilities and intrusion attempts. Information is analyzed to help avert or minimize disruptions to the telecommunications infrastructure. The results are aggregated and disseminated as provided by agreement among the ISAC members. In addition, the NCS hosts the NCC and is the lead agency for the telecommunications support functions under the Federal Emergency Response Plan. In that capacity, the NCC is specifically charged with assisting in the coordination of telecommunications restoration and provisioning during national disasters through government and industry cooperation on a 24-hour basis. NCS and the telecommunications carriers also collaborated on the development of the "Government Emergency Telecommunications Service" or "GETS", which provides government and industry personnel with key national security or emergency preparedness responsibilities with the ability to gain priority access to the public switched telecom network in times of significant network congestion.

There are two related reasons why we believe that the telecom-ISAC has been particularly successful. First, the Telecom-ISAC is funded largely by government ap-

propriations, so the core infrastructure and round-the-clock staffing is not borne exclusively by the private sector, as is the case with other ISACs. Second, government “partners” provide value back to the industry participants. First, the information-sharing goes two ways. The government routinely provides specific threat and alert information to industry representatives. Second, in real crises, the government NCC representatives quickly engage as ombudsmen on behalf of industry, helping industry gain access to impaired locations for purposes of restoration and recovery, and they represent the needs of concerns of the industry in terms of coordinating response. On September 11, 2001, the NCC helped network providers gain access to Ground Zero to restore communications, including arranging for military air transport for some of our key disaster recovery personnel who were stranded in California when commercial aircraft were grounded. The ability of government to deliver this kind of assistance, proven repeatedly in crises of differing degrees over the years, has led to an atmosphere of trust and cooperation in which we in industry have felt comfortable sharing sensitive information with the government and with our competitors in times of crisis.

This level of trust is essential because in order for information about security concerns and incident response activities to be useful to companies and to the government, it must be shared quickly. This need for expediency results in reports that are initially incomplete and potentially inaccurate, and there can be unintended consequences if the information is not treated with care. This trusted environment has also allowed industry and government partners to engage in periodic “exercises” to test the potential impact of different threat scenarios based on accurate network data from multiple carriers.

#### **The National Reliability and Interoperability Council (NRIC)**

Another example of the partnership that has worked and should be the model for any government and industry problem solving is the Network Reliability and Interoperability Committee (NRIC). First organized by the FCC in 1992, the NRIC was established following several telecom outages to study the causes of the outages and to make recommendations to reduce their number and effects on consumers. Since then, some 50 telecom carriers, equipment manufacturers, state regulators and consumers have participated. This has been a standing committee for over 10 years, and is a forum where industry and government come together for the good of the industry to work specific issues. Y2K was one such issue. NRIC VI is focused on Homeland Security with teams addressing both Physical and Cyber security. The product is a set of best practices (proven processes used in the industry) for service providers and equipment/software vendors to use to mitigate risk of attacks.

Another feature of NRIC is the monitoring and analysis of the performance of the public switched network based on reliability data collected during the last 10 years. The Network Reliability Steering Committee NRSC, a voluntary industry committee, reviews each outage report submitted to the FCC, looks for trends, publishes the results quarterly and annually, and looks for ways to improve the collective performance of the network. A new phase of this work, currently underway in the NRIC, is collecting similar outage data on wireless, cable and ISP networks in order to conduct data analysis, enable performance improvement, and develop new best practices. In leading this effort, the FCC has wisely recognized that to be successful, it must be: 1) voluntary; 2) developed by industry experts; and 3) adaptable by different network providers to reflect differing architectures and approaches.

#### **Safeguarding sensitive proprietary information:**

As a private sector operator of a major part of one of America’s most important critical infrastructures, we carefully safeguard all information about the physical locations, capabilities and components of our world-wide infrastructure. While some security experts discount the “security through obscurity” approach to risk management, I disagree. A July 9 Washington Post article describing the ability of a GMU graduate student to amass copious quantities of sensitive information about a vast array of critical infrastructure facilities highlights the danger of making sensitive information too easily available. In fact, we would suggest that if possible, this student’s report be provided by the Department of Homeland Security to the appropriate industry body, presumably the Telecom-ISAC, for analysis of its accuracy. It is in keeping with national security interests to assess the extent to which a motivated individual can develop a map of the infrastructure through compilation of publicly available information. The findings would be very useful in developing safeguards to prevent the continued proliferation of such information.

While this kind of threat clearly is of major importance for physical security, it also presents a very significant, indirect threat from a cyber-security perspective because the information could be used to launch simultaneous cyber and physical attacks,

which could result in exponential reductions in network capacity and potentially dramatic customer impact.

Despite these concerns, we are increasingly solicited by various governmental entities for very specific, extremely sensitive, proprietary information about our capabilities and maps of our network facilities and routes. States are attempting to compile lists of the critical assets of AT&T and other carriers for purposes of critical infrastructure protection. We are concerned about the breadth, open-endedness, lack of specificity, potential cost, and ability to safeguard and keep confidential any information that is provided. Neither states nor the federal Government should expect this information from network operators. First, security-related information that is provided to government entities outside the federal Department of Homeland Security may not be adequately protected from federal and state Freedom of Information laws. Even more importantly, it is not clear that information collected on a wholesale or generalized basis advances homeland security in any way, and may create greater risks to homeland security. In fact, proper analysis of any potential vulnerability requires a detailed assessment of the specific facilities of concern, the services they support, and the impact mitigation strategies applicable to those services. Instead of making arbitrary requests for massive downloads of extremely sensitive information, states should work with the Department of Homeland Security (DHS) and directly with critical infrastructure providers to determine what specific information is really needed and to establish coordinated processes and procedures. The DHS should be the focal point for the coordination across the regions, states, and municipalities, as well as across key industry sectors, to ensure that the information is useful, responsive, and properly managed.

**Expanding and refining the “public private partnership”**

We understand that the Department of Homeland Security, in coordination with the nation's governors, is updating and expanding the Federal Disaster Response Plan into a National Response Plan, and that private sector critical infrastructure providers will have the opportunity to provide input to portions of the plan that address how the private sector would respond in a national crisis. We applaud this approach, and look forward to continuing to work with the country's leaders, both public and private sector, to ensure that the private sector's views are considered and our capabilities are reflected in the evolving plan. I would also like to emphasize that a significant challenge during the recovery from the attacks of September 11 was physical perimeter control procedures that were changed as the responsible government authority shifted from local to state to federal control. As NSTAC recommended to the President, I also recommend that Congress task the Department of Homeland Security to partner with industry in developing a physical perimeter control plan to be part of the National Response Plan for use by all government authorities.

AT&T would like to particularly thank Chairman Thornberry, Congresswoman Lofgren and the Members of this Subcommittee for holding a hearing on this important issue. I offer AT&T's assistance to the Committee as well as my own, and I would be glad to answer any questions you may have.

Mr. THORNBERRY. Thank you, sir.

Finally, battling cleanup as they say, Tatiana Gau is chief trust officer and senior vice president at America Online. Thank you for being here and you are recognized for five minutes.

**STATEMENT OF MS. TATIANA GAU, CHIEF TRUST OFFICER  
AND SENIOR VICE PRESIDENT, AOL CORE SERVICES, AOL  
TIME WARNER**

Ms. GAU. Thank you, Chairman Thornberry, Representative Sessions, Representative Lofgren and members of the subcommittee. Thank you for the opportunity to testify before the subcommittee on the important issue of cybersecurity.

My name is Tatiana Gau, and I am the chief trust officer and senior vice president, America Online, where much of my focus is on cybersecurity, consumer protection, privacy and online safety.

At AOL we are committed to playing the leadership role on the issue of security. Employing our technology, tools and educational

resources we strive to provide secure products and services, to ensure a safe and secure environment online, and to educate our members to help them protect themselves.

As part of these efforts, we have developed extensive plans to address security issues in our products and services, our network and on the Internet.

AOL is working hard to implement recommendations in the President's national strategy to secure cyberspace that apply to our service. This strategy lays out some very important steps that the private sector should take and that AOL is undertaking to protect consumers.

We have designed elements of the next version of our software, AOL 9.0 Optimized, to fit the recommendations in the strategy. AOL embraces the partnership between government and private sector envisioned by the strategy, and we are committed to working with our vendors and competitors to strengthen security at the network and the end-user level.

Online security is an ongoing process.

At AOL, network security is an important part of the cyber safety equation. In order to prevent denial-of-service attacks and other intrusions, AOL, like many other ISPs, has integrated dynamic denial-of-service mitigation protection at all levels of our system which help us protect against attempted attacks.

We monitor our network for viruses and take both proactive and reactive measures to prevent, detect and eliminate them.

AOL also employs significant protections to safeguard access to member data. And we have incorporated many new safety and security features in our next client software, which is expected to be available later this summer.

These cutting-edge safety and security features include: a free firewall for broadband users provided in partnership with Network Associates; free and premium antivirus services which are automatically updated every time a user logs on to AOL; advanced spam filters; and computer checkups that enable our members to diagnose and fix security problems within their systems.

Through easy-to-use, behind-the-scenes protective measures and checkups, we are helping our consumers help themselves, especially in instances where the user may not know how to install or update security settings on their own.

Clearly no tools or technologies are useful unless consumers know about them and know how to use them. That is why AOL also undertakes significant effort to provide a wide range of educational resources.

For example, AOL's safety and security area online includes specific information about the security features that AOL provides and tips on how members can protect themselves against scams and viruses as well as how to protect their credit card numbers and passwords.

It also hyperlinks members to industry collaborative Web sites, like Stay Safe Online, GetNetWise, the FTC's information security Web page, for other specific suggestions and reinforcement of our messages.

In addition to informing our members about security risks and solutions, we recognize that online leadership means taking on re-

sponsibilities beyond the AOL community. To that end we have undertaken numerous initiatives such as joining with other leading private-sector companies to form the National Cybersecurity Alliance, in partnership with the federal government.

The Alliance Web site, [www.staysafeonline.info](http://www.staysafeonline.info), provides clear and concise consumer tips on information security as well as security background papers and research studies.

Just last month, in response to an Alliance study, and as part of our ongoing educational outreach, we launched a media campaign to inform high-speed users about the dangers of an unprotected broadband connection. The primary goal of this unprotected broadband media campaign has been to reinforce the message that Internet users need to be cyber secure citizens and ensure that their computers cannot be hijacked by hackers to engage in cyber crime.

Many of the initiatives I have outlined here involve close cooperation with our partners in industry and government and could not succeed without the existence of reliable processes for sharing information. Internet attacks can come from any part of the network of networks that constitutes the Internet and come in many different changing forms.

For this reason, AOL strongly supports the development of information-sharing and analysis centers—ISACs—and through these and other fora actively engages in sharing information about cyber-threats and-attacks.

And, because cyber-attacks can happen quickly and at any time, all ISPs should have a 24/7 point of contact within their company to work with other ISPs, other providers and governments to respond to potential cyber-threats.

We believe that government can play a valuable role working with the private sector in encouraging dialogue among all industry players to promote information sharing and helping to educate consumers and businesses. We look forward to working with the Department of Homeland Security to achieve this goal, and we applaud the creation of the National Cybersecurity Division last month to continue and expand on many of these public-private partnership objectives.

Thank you for the opportunity to be here today.

[The statement of Ms. Gau follows:]

#### PREPARED STATEMENT OF MS. TATIANA GAU

Chairman Thornberry, Representative Sessions, Representative Lofgren, and Members of the Subcommittee, on behalf of America Online, Inc., I would like to thank you for the opportunity to testify before the Subcommittee on the important issue of cybersecurity. My name is Tatiana Gau, and I am the Chief Trust Officer and Senior Vice President at America Online, Inc., where much of my focus is on cybersecurity. I oversee the integrity of the user experience, consumer protection, privacy, online safety, accessibility, community standards and policy, as well as crisis management and coordination for all of the company's brands.

At AOL, we are committed to playing a leadership role on the issue of security. Employing our technology, tools, and educational resources, we strive to build secure products, provide a safe and secure environment within which to surf the Internet, and educate our members to help them protect themselves. As part of these efforts, we have developed extensive plans to address security issues in products, our network, and on the Internet.

To succeed in the area of security, we work with our members to give them the tools and knowledge that they need to protect themselves. We cooperate with other

ISPs, mailers, and members of the computer industry on our plans and initiatives. We also work closely with the FTC, FCC, and other federal and state entities. Because of the nature of the Internet, we believe that only through cooperation among all the parties can we properly address cybersecurity as a whole, both for our members and the public in general.

AOL is working hard to implement recommendations in the President's "National Strategy to Secure Cyberspace" that apply to our service. This Strategy lays out some very important steps that the private sector should take and that AOL is undertaking to protect consumers. As I will describe, we have designed several features of the next version of our software, AOL 9.0 Optimized, to fit the recommendations in the National Strategy. AOL embraces the partnership between government and the private sector envisioned by the National Strategy, and is committed to working with our vendors and competitors to strengthen security at the network and end-user levels.

#### **AOL'S COMMITMENT TO SECURITY**

At AOL, safety and security are our top priorities. We have worked hard to develop a culture within the company where the starting point for all of our products and services is safety and security. However, online security is an ongoing process. It means providing consumers with easy-to-use security technologies, educating consumers about what to do to help keep their machines and the rest of the online community secure, controlling the use of our networks and keeping them safe, keeping personal information private, avoiding scams, and educating consumers about safe computing practices. Because we recognize that safety is one of the keys to instilling consumer confidence in the online medium and is critical to the continued growth and expansion of the Internet, we are working continuously to safeguard our members' accounts and computers and our infrastructure.

The AOL approach to consumer security is therefore threefold, with a focus on: 1) building more secure products and technology, 2) providing state-of-the-art security tools to our members, and 3) educating consumers-both at AOL and beyond-to keep security in mind while surfing the Internet. In each of these areas, we work with others in industry and our friends in the government in a partnership aimed at providing a secure network for all users.

##### **1. BUILDING SECURE PRODUCTS AND TECHNOLOGY**

Our company strives to develop and deploy the best security technology available. The AOL brand includes many products and services that many people do not realize are part of AOL, including AIM, WinAmp, and Netscape. We have invested in all of these products and services with the aim to provide the best security technology available for our subscribers.

We believe that network operators must make security a top consideration in every decision about their networks. We believe that they should monitor their networks for intrusions, apply all security patches for their software in an expeditious fashion, and employ a variety of other applicable best practices.

At AOL, network security is an important part of the cybersafety equation. We monitor our network for viruses and take both proactive and reactive measures to prevent, detect, and eliminate them. We have a dedicated team of network security specialists who are on call 24 hours a day, seven days a week to protect the security of our infrastructure. Moreover, AOL member-to-member communications take place within a controlled environment, and are facilitated over our highly secure data transit network.

In order to prevent denial-of-service attacks and other intrusions, AOL has integrated denial-of-service mitigation protections at all levels of our system, which help us protect against attempted attacks. AOL is no stranger to the cybersecurity fight. We are under almost constant attack from hackers and spammers who target our networks. To combat these attacks, AOL and other ISPs have designed Intrusion Detection Systems (IDS), which unobtrusively monitor corporate networks in real time for activity such as known attacks, abnormal behavior, unauthorized access attempts, and policy infringements. These systems can be used proactively to block certain types of infections and attacks. For example, ISPs can be configured to recognize and block inbound traffic that could otherwise infect AOL's corporate data systems. IDS also can be used to detect computer compromises through signatures that identify known hostile traffic patterns. When these compromises are detected in AOL's network, the IDS system generates an alert to the AOL security staff, which responds immediately.

When file attachments containing new viruses are reported to AOL by our members, a signature is built and passed on to anti-virus software vendors and our own IDS machines so that the viruses can be detected in subsequent attacks. We alert our customers as to how they can prevent further propagation of a virus and reach

out to other providers where we detect abnormal Internet traffic that may be generated by a virus.

AOL also employs significant protections to safeguard access to member data. AOL keeps passwords strictly confidential; verification of screen names and passwords is performed on AOL's secure servers. We recognize that a sound security system involves not only use of tools such as firewalls, intrusion detection systems, and anti-virus software, but that our employees play an integral role in protecting security. To this end, access to member data is granted on a need-to-know basis, and employees are extensively trained and screened prior to being granted access privileges. We also conduct periodic internal auditing of network records of data access to detect and promptly address suspicious activity.

## **2. PROVIDING OUR MEMBERS WITH SECURITY TOOLS**

We are particularly proud of the safety and security features of our new client software, AOL 9.0, which is expected to be available later this summer. These cutting-edge safety and security features include a free firewall for broadband users, free and premium anti-virus services, advanced spam filters, and a computer "check-up" that enables our members to diagnose and fix security problems within their systems. Some of these features have already been launched but will come together as a complete package in AOL 9.0.

To assist both our narrowband and broadband members, AOL runs a virus scan on all e-mail attachments that it receives from the Internet or that are uploaded from our members. If a problem is detected and we can fix the file we do so and deliver it to the addressees. If it is a Trojan horse, something that by its very nature cannot be fixed, we return the e-mail (but not the attachment) to the sender with a warning. However, e-mail attachments are only one way that a computer can get infected with virus. AOL, therefore, has a premium anti-virus offering that, after downloading a small program, will guard a subscriber's computer from viruses on floppy disks or CDs. In addition, every time a subscriber signs on to AOL, the virus definition file is updated with the latest virus definitions—the most important step in protecting your computer because more than 250 new viruses are released on the Internet every month.

In addition, AOL is providing broadband members with a customized firewall to guard against hackers and other unauthorized intruders by helping build a wall around the member's computer. The wall, when properly configured, blocks access to sensitive files, financial records, and personal data stored on the member's computer. AOL has teamed with Network Associates to provide free firewall protection.

We strongly believe that all users, whether an AOL member or a user of another service, should install, regularly update, and run anti-virus software at least once a week. If the user has broadband, he should also install and run a firewall. These two steps alone would dramatically increase the security of consumers' computers.

In addition, AOL has built in an array of security features to address the growing problem of spam. AOL already blocks as many as 2.4 billion spam messages in a single day. To empower our members and to track down and block spammers more quickly, we provide users with a "Report Spam" button on the AOL 8.0 software, which gives us rapid reports of spam that evades our filters. Building on the "Report Spam" feature and based on extensive member feedback, AOL 9.0 will contain unparalleled spam fighting tools that will make it easier for members to manage spam and to protect themselves from unwanted mail. These tools include very advanced filters, as well as a feature that will block images and URLs from unknown senders unless a member chooses to see them. This feature will help ensure that spammers cannot force e-mail that could compromise the security of members' computers. We also are working closely with Congress on legislative solutions to spam.

AOL 9.0 also empowers users to be proactive toward security by providing for computer check-ups. Through these easy-to-use check-ups and behind-the-scenes protective measures, AOL can diagnose and fix security as well as connectivity problems on a member's computer. We help the member help themselves, especially in instances where the member may not know how to install or update security settings on their own.

## **3. EDUCATING CONSUMERS AT AOL AND BEYOND**

AOL devotes significant time and energy to providing a wide range of well-placed education tools and resources that our members would find difficult to avoid. Because our members spend an average of 70 minutes per day online with AOL, we have ample time to remind them about security, and we do. This time online also has implications for the safety of the infrastructure. With more people staying online longer, those computers can be used to launch a distributed denial-of-service attack.

For this reason, AOL spends considerable resources to highlight safety and security information available on the AOL service. First, members can easily reach safe-

ty, security, and privacy information on the service with a toolbar button-which is always right in front of the member. Second, we have promoted and will be promoting even more educational material on spam and Internet scams with our Welcome Screen space. A recent Welcome Screen promotion on scam e-mails had the highest click-through of any Welcome Screen promotion (including those on Britney Spears) until we started our current promotion on spam. Spam is currently the number one area of interest to our members.

One important feature of our service is its Safety, Security, and Privacy area. Member security begins with educational tools that are clear, easy to find, easy to use, and easy to customize. Collectively taking care of our community, this site urges members to "protect your home computer and the nation's Internet infrastructure." The site includes specific information about how members can protect themselves against scams and viruses, as well as how to protect their credit card numbers and passwords. It also hyperlinks members to industry collaborative sites like "StaySafeOnline," "GetNetWise," and "Site-Seeing Tips: Travel Insurance for Cyberspace" for other specific suggestions and reinforcement of our messages.

Another key feature of our service is AOL Keyword: Help. This feature provides a resource for members who need assistance on any topic, including security. This process is easy to navigate, clear and simple to understand. At Help, one of six listed topics is "Online Safety." Clicking this link gives the member online safety sub-topics to choose, including information on protecting your password, avoiding computer viruses and spotting scams and schemes. Clicking any of these choices gives the member a menu of related short, simple, useful articles such as "Password Requests in E-mail," and "Password Stealing Schemes."

In addition to providing many avenues for our own members to be fully informed about security risks and solutions, we recognize that online leadership means taking on responsibilities beyond the AOL community. AOL feels keenly an obligation to use our resources wisely for the benefit of all consumers in the online world. To that end, we have undertaken numerous initiatives.

For example, we have joined with other leading private sector companies to form the National Cyber Security Alliance, a unique partnership with the federal government that fosters awareness of cybersecurity through educational outreach. The Alliance website, <http://www.staysafeonline.info>, provides clear and concise consumer tips on information security. AOL is proud to have participated in the design of that site, to be hosting it on our web servers, and to be dedicating substantial resources toward driving traffic there.

To gauge consumer attitudes toward and readiness regarding cybersecurity, AOL has commissioned studies independently and with others in industry to help identify areas where efforts and initiatives can further enhance security. We use the results of these studies to tailor solutions to members' attitudes and practices. A recent study conducted by the Alliance demonstrated that the overwhelming majority of broadband consumers lack basic protections against the dangers of an always-on connection to the Internet. The study revealed that most consumers do not realize that they lack those protections or that their computers and personal information are at risk.

In response to this study, and as part of our ongoing educational outreach, we launched a major campaign in June to inform high-speed access users about the dangers of an unprotected broadband connection. The primary goal of this Unprotected Broadband media campaign has been to reinforce the message that Internet users need to be cybersecure citizens and ensure that their computers cannot be hijacked by hackers in cybercrimes.

#### **4. THE IMPORTANCE OF INFORMATION SHARING**

Many of the initiatives we have outlined above involve close cooperation with our partners in industry and government and could not be successful without the existence of reliable processes for sharing information. Because Internet attacks can come from any part of the network of networks that constitutes the Internet and come in many different, changing forms, information sharing regarding security threats is essential to good cybersecurity. For this reason, strongly supports the development of Information Sharing and Analysis Centers ("ISACs"), and through these and other fora actively engages in sharing information regarding cyber threats and attacks.

This cooperation has proven very important to the continued stable operation of the Internet. For example, in February of 2000, the ISP industry worked together to combat the largest attack on the Internet to date by a single individual in Canada who was able to organize a large scale denial-of-service attack on several large websites, temporarily knocking them out of service. As the attack occurred, the large players in the ISP industry quickly communicated with each other, through informal technical contacts, to isolate and locate the source of the attacks. As a re-

sult of the industry's quick response, service to the websites was restored in a matter of hours, and the functionality of the Internet as a whole was never interrupted.

This type of response is typical in the ISP industry, and these well-established informal procedures and responses proved to be effective in remedying subsequent attacks on the infrastructure, such as NIMDA and Code Red viruses.

When our IDS system detects or we receive reports of new viruses, we build a signature and pass along to anti-virus software vendors as well as our own IDS machines. We also reach out to other ISPs when we detect abnormal traffic patterns that may reflect a virus or hacker attack, and have a Cybersecurity team on call 24 hours a day, seven days a week available to address indications or reports of security threats. Indeed, because cyber attacks can happen quickly and at any time, we believe strongly that all ISPs should have a similar 24/7 point of contact within their companies to work with other ISPs to respond to potential network abuses.

Information-sharing can also help on the law enforcement side of the cybersecurity equation. AOL works closely with law enforcement and other government agencies to deal with threats to the critical infrastructure, even when those threats may not directly affect AOL or our members. AOL has a dedicated team of professionals, including former prosecutors, who work with law enforcement in investigations of cybercrimes, including hacking and other security threats. We cooperate with authorities not only in responding in a timely fashion to their requests for information during an investigation, but also pro actively in alerting law enforcement to potential network threats. AOL has worked closely with government and law enforcement to identify and locate major hackers whose actions have threatened the Internet, including the creator of the infamous Melissa virus.

We look forward to working with our colleagues in industry and government to build upon these existing mechanisms for cooperation and information-sharing, and to ensure that the lines of communication are open and clear.

#### **THE ROLE OF GOVERNMENT AND PUBLIC-PRIVATE PARTNERSHIPS**

We believe that government can work with the private sector in the following key areas of cybersecurity: 1) encouraging dialogue among all industry players to promote informationsharing; 2) educating the public about staying alert to potential network abuses; and 3) promoting active cooperation between industry and government in finding and apprehending hackers. Many of the initiatives we outlined above have involved close cooperation between government and industry players in these areas.

With responsibilities for cybersecurity now coming under the primary purview of the Department of Homeland Security's Directorate for Information Analysis and Infrastructure Protection, we applaud its creation of the National Cyber Security Division (NCSD) last month and believe it can continue and expand on many of these public-private partnership objectives. We look forward to working with the NCSD, particularly as it seeks to:

- identify risks and help reduce vulnerabilities to government's cyber assets and coordinate with the private sector to identify and help protect America's critical cyber assets. As previously stated, government can play a very valuable role in keep the lines of communication open and clear about cyber threats and cybersafety;
- oversee a consolidated Cyber Security Tracking, Analysis & Response Center (CST ARC), which hopefully will serve as an effective, single point of contact for the federal government's interaction with industry and other partners on a 24x7 basis. The CST ARC should work closely with existing ISACs and should seek to develop tools to increase communications among all players; and
- create cybersecurity awareness and education programs and partnerships with consumers, businesses, governments, academia, and international communities. In coordination with the National Cyber Security Alliance and its StaySafeOnline campaign, and other organizations, the NCSD should seek to advance the development and expansion of education programs without delay.

We look forward to seeing DHS's execution of the actions and recommendations outlined in the National Strategy to Secure Cyberspace, and will support those efforts as we continue to work closely with government and law enforcement in minimizing threats to our cybersecurity.

#### **CONCLUSION**

We applaud the Subcommittee for its examination of these issues as companies such as ours undertake significant efforts on behalf of our members and the Internet as a whole. We will continue to work hard to implement recommendations laid out in the National Strategy in our products and our outreach initiatives, and encourage other companies to do so as well. We are deeply committed to addressing cybersecurity in partnership with government and with our suppliers and others in

our industry. We look forward to continuing to work with Congress, the Administration, and others in industry toward ensuring cybersecurity.

Mr. THORNBERRY. Thank you.

It is a little bit frustrating from this side of the dais because I think the subcommittee could spend an entire hearing with each of you. And yet what we are trying to do is also get our arms and brains around the larger problem, the overview. And so we appreciate each of you being here today.

I want to mention before we turn to questions that toward that end this subcommittee is sponsoring, with CRS, a workshop on cyber-security, and I would encourage all members to have their staff members attend. It is Monday, July 21, in the Cannon Caucus Room. Ms. Lofgren and I have sent information on this to each of your offices. We have some fine folks who are there and I would recommend that you send your people.

I would like to start with a kind of a broad overview question addressed to each of you. And a number of you have talked about this in your statement. But, again, in the interest of trying to see if there is consensus and in broad form where we go, I would like for each of you to briefly address this question. We are not going to have time to get all into it, but we will go back.

And here is, I guess, my question. The market is driving each of you towards some measure of greater security. First question is, are you comfortable that that market-induced level of security is sufficient for our nation's security or is something more required than where the market is going to take you?

Secondly, if you think something more is required—and I don't assume that—but if you think something more is required, then just in rough outline what is the federal government's role in achieving that extra measure beyond which the market allows you to go.

Again, I would ask each of you to be relatively brief in your answer, because I want to turn to other folks, but that is kind of the big question that this subcommittee is grappling with. And so I would like to just go down the line.

Mr. Reiting, if you would start?

Mr. REITINGER. Thank you, Mr. Chairman. I will try to be very brief.

I think the market is going to go a long way. This is a very innovative industry. And as you heard from the panel today, across the industry we are seeing security innovation.

It is possible that in selected areas the market will not go as far as the nation needs for national or homeland security purposes. I have two points on that.

One, you can't look at that broadly, though. In other words, the market may not go far enough in a particular place, or in another particular place or sector. So I think it is less a broad question and more a particularized question.

Second, it is dynamic. In other words, the question is not where is the market now, but where is the market going and where do we need to be? Do we need to look at the direction we are going in.

Second point, even if the market is not going to go as far as we want to go, I would urge policy makers to move in as, I believe my

estimable colleague Whit Diffie said, as tailored a fashion as possible. Just because the market may not go as far as you need for national security doesn't mean to leap to regulation or some other mandatory step.

I think one of the critical functions for the new Department of Homeland Security is to take a very close look at where the market is going, figure out what it is going to do, where there may be gaps, and then figure out the best and least intrusive way to close that gap. And I think some of the suggestions we would have I stated in my written statement and I outlined for the committee and won't repeat.

Thank you.

Mr. THORNBERRY. Thank you.

Mr. Diffie?

Mr. DIFFIE. I think I will take it for granted that there is some role for government in this and just spend a moment or two just looking at what that might be.

I think it is important for the government to do those things that it is uniquely qualified to do. So, for example, the government has access to information that is not available or not as readily available in the private sector. And so, as I said in my testimony, I believe that a follow-up mechanism for measuring the actual security of systems in operation should be used to validate the certification mechanisms.

This turns on the fact that the intelligence information needed to do that is very hard for industry to get because individual pieces don't want to share it and they share it more readily with the government.

I also believe the government has played a very important role in standardization. I cited the advanced encryption standard. If it is anything like as successful as its, I believe, more controversial predecessor, the data encryption standard, that will be something that the fact the U.S. government took this on as a standard will have a transforming effect.

Finally, there is government's incomparable role as a customer, both in the sense that the government could perhaps show more foresight in putting security forth as a requirement for the systems that it uses but also in a unique ability to engage in certain large purchases, so to speak. So, one of the problems—we have had a long discussion of why public key infrastructure has not developed as well as many of us hoped. And I believe at root that is a capital development problem. That is to say, like a telephone infrastructure, a keying infrastructure becomes more valuable, the more of it there is. And so it is hard to get it started.

So, if you contrast general government and civil sector keying activities with those of the Department of Defense, which has a focused mechanism for putting out up-front development costs, you see that they got much better results in a shorter period of time.

So I think the government needs to consider what major steps like that it might take.

Mr. THORNBERRY. Thank you. Dr. Lowery.

Dr. LOWERY. I am wondering if there will be much left to say by the time you get to the end of the row because many of the themes that you have heard expressed so far to my right we also concur

with. In particular, government's role as a customer is one that we see as extremely important. You have a lot of opportunity to give us input through our direct relationship with you as a customer of Dell, for example, to tell us what it is that you want.

And the CIS benchmark offering is a prime example of this in action. This is a result of government customers asking for that. So, as a customer, I think you have immediate impact to how industry works through market forces.

The coordinating role of government also should be reemphasized because since we do believe in standards or where this is going to happen, the consensus that needs to be driven here, a coordinating role is important to make that happen. And I think that government helping to arrive at standards is an important function that you can provide. And we would like to see more involvement in helping to coordinate the standards that are already being developed through the market.

Mr. THORNBERRY. Thank you.

Mr. Adelson, is market enough? And if not, where does government fit?

Mr. ADELSON. I believe market drives much of the end-user requirement, end-user type of applications and tools. While government can certainly advise and inform the service providers to provide those tools, market will only go so far as to, say, create my end-user environment, something from Microsoft, something from AOL.

At the network infrastructure level, for example, if two networks have authentication when they speak with other, users never see that. They don't know if it is on or off. And so, in order to get network infrastructure going, you have to have certifications and standards, create some kinds of best practices, check against them, and then be able to advise the user community that a network has met or not met those standards.

Mr. THORNBERRY. Thank you.

Mr. Ianna.

Mr. IANNA. Answer to the first question. I think that the market will take it a long way but not all the way. And I think the government can help here.

And I would liken this back to when the FCC and the Telecom industry created the network reliability council. I there were some failures in the industry, local carriers, long distance carriers. And I think they were dragged in front of a hearing, and were asked two basic questions.

Number one, how reliable is the public switched telecommunications network? And there was not a lot of good information to give that answer. And if you couldn't answer the first question, you certainly couldn't answer the second one, is it getting better or is it getting worse?

Forming the network reliability council brought all of the participants in the industry together, NRIC as it is now called.

And we now have some 44 quarters worth of data broken down amongst the components, the physical components, of wire line networks as to what causes failures. And we know how reliable it is and is it getting better or worse and what is causing a particular problem.

So I would suggest that the way that we approach this—is, to have a voluntary public forum that we could share information, best practices and the like and that we set a standard to answer the question: How cyber secure are we? And there is going to be a metric around that. And is it getting better? Is it getting worse? Because it will continuously change. As we interconnect one network to another network, if somebody introduces a new application, the holes or the opportunities for hackers to get in and do something will change continuously.

By the way, I think you could also answer the question amongst different industry segments, the financial industry, the water industry, the power industry. And each one of those can focus on their own mission-critical services and how cyber-secure they are and how they need to be. And we could share information amongst those ISACs too.

Mr. THORNBERRY. That changing nature is part of the challenge for government because we don't change very fast, particularly when we are talking about laws and regulations. So I think that is a good point that several of you made.

Ms. Gau?

Ms. GAU. I have been with AOL since the mid-1990s and never has there been a time where I haven't had to argue until I was blue in the face about the need and the good business sense to include security in our products. Our consumers are demanding it now. Extensive research that we have done shows that it is first and foremost on their minds when they are surfing the Internet, especially if they have family involved.

And they may not be thinking about the nation's critical infrastructure in that context, but they are thinking about how to be safe themselves and how to protect their point of vulnerability. And obviously, they have the buying power.

Well, consumers are not the only buyers out there. As some of my colleagues have mentioned, government can play a role here in really driving the market for more secure products. One—a similar situation might be with Section 508 of the Americans with Disabilities Act which requires that companies include accessibility in their products if they are going to sell to the government. Similar types of approaches could be taken in the area of security.

With respect to what more could the government do, I would go back to the mission of the National Cybersecurity Division and to homeland security in general in this area with respect to information-sharing, providing those of us in the industry, those of us that are working to keep the critical infrastructure up in place with information that we might not be able to easily obtain elsewhere; to provide for research and development in areas that we are not able to. And to also work to educate all users, consumers, businesses and other government agencies alike about the need for cyber-security.

Mr. THORNBERRY. Thank you.

Ms. Lofgren?

Ms. LOFGREN. Thank you, Mr. Chairman. This is a very helpful panel.

And actually, if I am listening to you, I am hearing broad agreement on many themes: that we do need standards. We need ac-

countability towards those standards. We need a role for government in coordination and maybe assisting in the development of those standards, additional research.

I am glad, Mr. Ianni, that you mentioned the physical infrastructure issue because that is also—I don't want to belabor that. But that is something that we—you know, we are thinking hackers, but actually the tradition of terrorists has been guys with bombs. So we should not overlook that element.

I have a question because Mr. Diffie mentioned that we do now will have a downstream effect. And I think about that all the time, that if we make a misstep now that it will have an impact, you know in 10 or 50—my children will live with the mistakes that I make. And so I especially want to avoid them.

And while we are focusing on security, which we must do, I am eager to hear from you, what is the worst thing we could do as the federal government that would either impair our security, but also impair our liberty in the future? I am concerned about what we might do now that would impact the architecture of the Internet to the detriment of our free society. And I am wondering if you have thought about those issues and what your thoughts might be. Each of you, starting with Mr. Reitingner

Mr. REITINGER. Thank you, Congresswoman. Although it is a little unfair for me to go first on each of these. I will be very brief so I don't cut folks off.

I would say I think the worst thing that you could do is something that would impair security and privacy innovation. Doing something in such a way that the ability of industry to respond to the increasing market demand for security and the increasing need for homeland and national security, that ability would be impaired in some way.

Mr. DIFFIE. I guess my greatest concern is that these technologies will get bottled up and become the properties of—to give the jargon, certain elites, in the way that say, drug development is now regulated. I think it is very important that people continue to own their own computers, genuinely to own their own computers, to have the root authority and the actual power to control what their computers do. So that we get security sort of by an aggregation from the ground up of all of the individual citizens, rather than something imposed by some government-industry security mechanism that restricts either security practices, security uses, or in general, the use of computers by the citizenry.

Dr. LOWERY. I think anything that you do which does not allow for the fact that security is a moving target is going to be ill conceived. It is a changing landscape from day to day.

So anything that is done above and beyond what customers are asking us to do, I think has to be very carefully considered, because ultimately, as time moves forward and we are looking back on what we are deliberating today 15 years from now, we very well may say, How could we have foreseen this happening?

So we have to be very open minded about what could happen in the future, and not kid ourselves that we have all the answers today.

Mr. ADELSON. I think anything that government does that would slow down first response, and from, you know, that if, your good

intentions aside, monitoring or controlling the "Internet," with quotes around it, you know, is something that is far beyond the scope, and if you tried to implement such a thing, I fear that the Internet itself would actually be at increased risk toward our, you know, how fast you get back up after a national crisis.

Mr. IANNA. I think the worst thing that the government could do is not listen to the industry participants as to what they are capable of doing, and what can be done in a timely and cost-efficient manner.

I go back to some of the NRC days, where we were trying to define a failure. And if you ask a consumer group, they may come up with something that says, Well, this is a failure, and every time you have this failure you need to file a report.

We would have cut down acres of trees and buried Washington in paper and not improved the state of reliability had we adopted some of those that the industry said, This can constitute a failure, and this is what we want to improve. We work together in a true partnership.

I really believe that all of the industry participants in that case, in telecom, although we were fierce competitors, came together in the best interests of the country.

So listening to the participants about what is doable and what can be done quickly and cost-effectively, I think, is very important. Not listening to them, I think, would be a very big mistake.

Ms. GAU. Well, I have to echo all my colleagues' comments, particularly in the area of developing standards that might be obsolete by the time they would be published, because security is a moving target, and it is an ongoing process.

Additionally, I think, one of the worst things government could do would be to not engage and further strengthen relations with the private sector.

There have been ongoing dialogues, AOL have very close working relationships with government and also with law enforcement at the state and local levels, and we are engaged in a continual dialogue.

But anything that would hamper our ability to respond, whether it is some type of system where we have to go through a central control without being able to first focus on what we need to do as a company to get our business back up and to be able to provide the service to our customers would be a mistake.

Mr. THORNBERRY. The gentleman from Texas, Mr. Smith.

Mr. SMITH. Thank you, Mr. Chairman. Mr. Reiting, let me address my first question to you and ask you to call upon your experience with the Department of Justice, where you served prior to joining Microsoft.

There, according to your bio, you were a prosecutor of computer crimes. One of the frustrations we have on this committee, and I have to say we have in on the Judiciary Committee, as well, is not being able to quantify the number of computer crimes, not knowing how many are committed, not knowing what the trends are, and therefore, not being able to necessarily address the problems as much as we should.

As you know, when computer crimes are prosecuted, they are kept track of by statute not by type. What can we do to get a better

handle on the types of computer crimes that are committed, how many are committed and what the trends are?

Mr. REITINGER. Thank you very much, Congressman.

I think your frustration is widely felt. One of the concerns—and you will see in the opening of my written statement, as I think in prior testimony the committee has seen, there is a general sense that we don't really know what the scope of computer crime and computer damages are. We actually don't have a statistically rigorous measurement of the amount of harm from computer crime and computer attacks.

There are government agencies that do that sort of thing, the Census, the Bureau of Justice Statistics. I would think that having a statistically rigorous analysis of the amount of harm that our economy faces as a result of computer crime would be a very valuable thing and help close what I think of as the knowledge gap that we face in addressing questions in that area.

Mr. SMITH. I agree and I think that is exactly what we need to do. And I will try to engage in some discussions with the various agencies to try to collect that information for the reasons that you stated. Thank you.

Dr. Lowery, in regard to your testimony, you mentioned some of the initiatives that Dell has taken as far as systems security goes. Would you go into a little bit more detail of specifically about what Dell has done that you find effective.

Dr. LOWERY. Yes, I would be glad to.

Dell has responded to customer input, specifically from our federal customers, to deliver from our factory directly to them Microsoft Windows 2000 installed on Dell computers, specifically the Optiplex, Latitude and Precision Workstations, that are already set with the configuration settings from the Center for Internet Security, which I mentioned before.

The reason that we have done this is purely because customers have requested it. Also, we see it as something that can be made available to all of our customers. It is not something that is restricted to our federal customers. We think that everyone can benefit from it.

So this is an example of industry best practices as they exist currently, today, that we can bring to market with very minimal lag time because of our direct model. We build—most every system that we ship is custom built to that particular customer's order. And so as soon as we have new information that impacts product safety or security and we are able to get that into the product and into the factory, it is in our customer hands typically in five to 10 days after that as we start shipping it.

So that is why we have taken that role. We can deliver that technology fairly quickly to our customers that have requested it.

Mr. SMITH. Thank you, Dr. Lowery.

Mr. Reiting, let me go back to you and Ms. Gau. Both of you have had extensive experience dealing with the federal government. We have heard in response to some earlier questions that we need to establish a better relationship with the federal government. We need to do more listening, and so forth. Specifically, though, how do you think the federal government can better, or more enhance cybersecurity?

Ms. Gau, let me begin with you.

Ms. GAU. At the risk of sounding repetitive, I am going to go back to the information-sharing, the research and development, coordination with private sector and education components that actually form the mission of the National Cybersecurity Division.

One of the areas that we are looking at right now in terms of the industry is information-sharing with each other and how we can continue to improve on those processes that already exist, such as 24-7 contacts that exist amongst the players in the industry. And taking that a step further, really having that kind of cooperative relationship with government at the DHS level in the National Cybersecurity Division is something that I would very much look forward to.

At this point, we are still developing our relationship with DHS and I look forward to seeing the Cybersecurity Division get going, so to speak, and engage us more actively.

Mr. SMITH. Okay. Thank you.

Mr. Reitinger?

Mr. REITINGER. Thank you very much, Congressman.

I will also—I think the main points we have hit on and Ms. Gau also retracked there—let me touch on one point on information-sharing. There is an anecdote I have heard about something that occurred long ago, before the IT ISAC in particular was formed, where my boss' predecessor, Howard Schmidt, got a call in the middle of the night from the network operation people who said we are seeing a spike in network activity. He came in and he saw that there in fact was an issue and started calling his colleagues, including a colleague from Sun.

They were able to sort of quickly see that this spike was occurring across the networks and take some action. In particular, Howard was able to reach out and talk to people at the Department of Defense, and as a result, a lot of DOD computers got protected as a result of that.

This goes to show that we already have a lot of ad hoc and very valuable information-sharing that is taking place. What we need to do now is put that on rails, make it a part of business processes for both government and industry so it becomes a part of how we do business. And the government, I think, can help a lot in that regard, in particular in some of the ways Mr. Ianna was referring to.

Mr. SMITH. Thank you, Mr. Reitinger.

Thank you, Mr. Chairman.

Mr. THORNBERRY. Thank you.

The Chair's intention is to call on members in the order of appearance at the hearing. And I will now call on the gentleman from North Carolina.

Mr. ETHERIDGE. Thank you, Mr. Chairman. Let me thank you and the ranking member for holding this hearing, and more specifically, for our witnesses being here today, because I sit here and think of so many questions, so much information and so little time on such a critically important question.

Mr. Reitinger, let me ask you the first one, because I am going to go from your written testimony, if I may, and then I will come

back and ask the others. The next time I will go in reverse order from the other end. But yours first.

You stated that cybersecurity remains an interagency problem, as you said earlier, and that a key role for DHS and the National Cybersecurity Division is building industries for effective government action in helping other agencies develop procedures that support homeland security.

What has the department done thus far to fulfill this role? And have its efforts produced results that industry is feeling?

Mr. REITINGER. Thank you, Congressman.

I might be the wrong person to ask that question to. The people who could best answer it would be in the department.

I am very encouraged by a lot of the activity that the department is undertaking. I think they are very new. They were only officially stood up less than six months ago. But listening to the things that they are saying, particularly Assistant Secretary Liscouski, on the issue of cyber-security, I am looking forward with hopeful expectation to the things that they are going to accomplish.

In particular, one of the things that I think they are doing is focusing on deliverables, getting things done in both the short term and the medium term as they look towards the long term.

I think there is a tremendous problem there. There are a lot of government stovepipes that need to be tackled. And I think the entire department needs a lot of help from across the bureaucracy and from this committee. But I feel very hopeful about it.

Mr. ETHERIDGE. Thank you. Want you to understand, I asked you that question because you have been inside and now moved outside, and I think it is critically important to hear your views on it.

Let me start on the other end and ask this question of each one of you very quickly, because each one of you touched on about the security issues that you are employing that you have ramped up.

And my question is, what event or events prompted the additional focus on security from your strategic standpoint as an industry? Because different ones have talked about the customer demands—that does it. Was it customer demand or was it an attempt to differentiate between products or some other events? Because you have shared with us the need for industry to be given a goal, but at the same time industry's going to take certain actions.

It would be of interest to me and I think to others on this committee to know some of the things that have driven that.

Ms. GAU. As a consumer-facing business, the AOL perspective is going to be geared, obviously, towards what we see with our consumers.

Whereas there have been the early technology adopters, as well as other people out there in the marketplace that have always been concerned about security, I would say that it was probably right around the time of the Melissa virus in the year 2000 when the mass market of consumers all of a sudden realized that, My gosh, a virus, and the whole story of how it propagated and how the guy then got caught and the cooperation that was entailed in catching the guy—it really all of a sudden woke people up.

And it was about the same time that also there were the attacks against eBay and a number of other major providers that were

taken down for a brief period of time, as well as some privacy breaches, some high profile privacy breaches that took place that year.

So I would say it was really in 2000 that we started seeing our consumers identifying safety and security as a top priority for them in the security research or general research that we do on a routine basis to understand our customers.

Mr. IANNA. Actually, it starts from customer demand, but that only starts from the base of what you know and what you are trying to protect against. For example, in a data network you are saying, I am trying to make it as reliable as I possibly can. People know about cable cuts, they know about software failures—trying to make sure that this network is four nines of reliability. All of a sudden some other new thing comes up, somebody does a distributed denial-of-service attack, and you are hosting that Web site in your network. You now have to be aware of the fact that this goes on and how do you mitigate it.

So it is not only customer demand but it is an event that occurs that is a new form of failure that you very quickly have to adapt to.

And unfortunately, as networks get more and more sophisticated—for example, let us say for example in data networks now, Wi-fi becomes a very popular form of access. I guarantee you we will see different types of failures and different types of potential intrusions in gathering information in that network than we have seen in other networks, maybe because of the unsecure nature of transmitting some of that information.

So it is the baseline of what you know always augmented by something new happening and customers saying, “I don’t want that to happen to my application. What are you, AT&T, what are you, service provider, ISP, doing to prevent that from happening again?” And that is what drives our continuous development.

Mr. ADELSON. I will speak to the physical components, since that is our area of speciality.

There was no specific event which changed the focus on physical security for us. I know back in 1996, I worked at Digital Equipment, in their research, and what we found was that the participants—and infrastructure radically changed from 1996 to 1997, and started to include companies like Alta Vista and Yahoo and Google, as well as the network service providers. Their requirements for physical security had commerce behind it, and it changed all of the focus.

And so, for example, exchange points moved from a central office to a robust physical infrastructure. That is really the closest thing to an event—it is really a market shift that focused our change.

Dr. LOWERY. Congressman, I would say that I perceive no specific event, but instead a succession of events that are also progressive, kind of ramp-up.

And also, as Mr. Diffie mentioned earlier, we are making a transition to more virtual world. And so it is becoming more important, and becoming something that we rely on increasingly. And this has been happening over the past three or 4 years. The time lines you have already heard.

So that does drive customer demand. As customers become more aware of how much they have invested in these technologies, and how much those technologies impact them personally, they start making more specific requests.

And as I said, we are always open to our customer input. That is what we are looking for. We look to them to help us make a determination as to where we go next as far as what we should be doing with our products.

Mr. DIFFIE. Well, he stole my line. I thought I was going to be first to say that I couldn't remember any explicit event.

As I go back over the half dozen things I can list, which seems to be significant Sun contributions to security—client server computing Java, hardware domaining, trusted Solaris—my sense is that they are the responses to our perception of our customers' needs in security, as opposed to their desires in security.

So, for example, with the rise of the World Wide Web, the development of a computer language intended to have security with mobility—in this case, mobility of code—was intended to enable the sort of business development that we saw.

And I think that is the kind of reflection that is always going to be required in this area, that you are never able to determine security requirements merely by market survey.

Mr. ETHERIDGE. Thank you, Congressman.

Rather than listing a specific event, I will briefly mention three factors that I think play outside of customer demand, one of which relates to what Mr. Diffie was just talking about.

First, I think there is a business imperative to build trust. Security is in a sense less a size of the slice of the pie issue as it is a size of the pie issue.

For all of us to do better and be more successful, we need people—and for society to be more successful—we need people to utilize information technology broadly. That is not going to happen unless people trust information technology. And so we need to accomplish that.

Second, September 11. September 11 taught us we need to worry not just about the foreseeable, but also the unforeseeable.

And third, and this is a point related to what was just talking about: social responsibility. With market share comes responsibility. And we as large and important corporations have a responsibility to look towards protecting the security and privacy of our customers.

Mr. THORNBERRY. Thank you very much.

Thank you. Chairman Cox.

Mr. COX. Thank you, Mr. Chairman.

I want to thank this panel for being exceptionally educational and for your willingness to devote some careful thought into providing your fair testimony even before you got here and, of course, for your years of experience that enabled you to do that.

And I want to thank the chairman and the ranking member for organizing this particular focus on cybersecurity. As members of the panel know, in organizing this Committee on Homeland Security, and indeed, in organizing the Department of Homeland Security last year, the Congress had it in mind to pay particular attention to our information infrastructure. And this subcommittee is

the only subcommittee in either the House or the Senate devoted to cybersecurity.

I make the point because so much of our focus on what we now call homeland security, on fighting terror, is really coming to grips with technology, whereas in the 20th century, only nation states could pose WMD threats to us; in the late 20th century, we found that such dirt-poor nations as North Korea could pose similar threats. And now we are finding that terrorist bans, and ultimately I am sure we will come to the conclusion in the 21st century, that individuals will find their own capacity to harm civilization levered by psychology in the same way that this technology is improving our productivity in all other peaceful aspects of our existence.

And so I want to make sure that as we organize the Department of Homeland Security, we are focused not just on, for example, the Internet the way we know it today but on where this technology is headed, because 10 years ago if we would had this hearing and asked these questions with all that time to prepare, we still couldn't have prepared ourselves because so much of what we have today was unknowable at the time. And we want to make sure that in the future we are nimble.

So in matching the strengths and weaknesses of the federal government, which we have all agreed today need to be a partner in this venture with those of the private sector, I find that one of the federal government's characteristics is extremely troubling. And that is that it tends to be ponderous and sluggish in its movements in developing regulations or in implementing its policies. Whereas what typifies not only the private sector but, in specific, the technology industry is lightning quick ability to change. And this change is going on all around us, not just our nation, but around the world.

And so, my question is as we have gone from, for example, code red 2 years ago to slammer this year and we have got our reaction time to a matter of minutes, and we may be looking at even seconds, when what you are asking the federal government to do is help post best practices, how do we deal with the fact that it might take too long for the federal government to be the clearinghouse for this information?

And anyone who wants to jump at that is welcome to do so because you are all expert in this.

Mr. DIFFIE. Well, I will take a brief crack at it and say I think that the federal government should not be apologetic for being ponderous and slow. It is running the largest enterprise in the world. And I don't think if we look at the record that we would see, in cases where it is active in haste, it has necessarily acted very wisely.

I think the important thing in here is that there are long-term principles. Federal legislation must recognize the principles, speak to the principles, speak to provision of resources, and certainly weave the rapid reaction much further down the chain from Congress, perhaps to parts of federal agencies and to industry and individuals.

Mr. COX. Well, that certainly reflects my views, particularly when it comes to writing legislation. I want to be sure as a norm here in Congress that we try not to write technology into the law,

because ultimately the lawyers will then make sure that in order to comply with the law, you maintain the technology that is written in the statute.

And that will be a very, very bad world indeed. And so, I think your recommendation is getting us on the right track. I would be happy to hear further.

Mr. IANNA. Yes, I think the answer to that question or a answer to that question is there are many solutions to a problem of sharing information. For example, the Telecom ISAC, we have to be very comfortable with that one. It has been a good government/industry partnership.

I think the thing that we could be ponderous on is that there are many good solutions, and deciding which is the right one, we spend too much time on. I think they are all about 80 percent right.

And I think we need to spend more time on taking a good example of what works and then applying that to other industries not and worry about not making the right solution, but making the solution right, and leave the quick, rapid response to an ISAC or to an information sharing way lower down in the chain, but get the people and the participants participating in that very quickly and define what you want to protect and how you want to define your measure of success very quickly.

And just say, for example, if you are protecting water, what is our critical systems that we want to have? What is the level of cybersecurity we need around those? Let the industry participate in that. And then, further down the chain, let them go implement those solutions.

And then you will have to continuously look at it, because threats will change, lots of things will change, networks will change, but you will have a history, then, of are we getting better or are we getting worse? And that is the key.

Mr. THORNBERRY. Mr. Reitingger?

Mr. REITINGER. Just briefly, chairman, thank you.

I think that this is a—cybersecurity is a network problem much like the Internet, and requires a network response. The government has some very important nodes on that network, with some strengths and weaknesses, and probably needs to concentrate on the things it does well and must do, as Whit was saying before.

Within DHS, I think it needs to concentrate on three things: people, process and technology. And I think of those three, they are all important, just to expand a little on process. There are a lot of government business processes that are no longer well suited to protecting homeland security in a new environment. And DHS needs to lead that transition and incentivize—I know it is a private sector word—but incentivize that transition within government for processes that effectively protect homeland and national security.

Mr. COX. I thank you, Mr. Chairman. My time has expired.

Mr. THORNBERRY. I thank the Chairman.

Ms. Christensen?

Mrs. CHRISTENSEN. Thank you, Mr. Chairman. I want to welcome the panelists. We have had some briefings on cybersecurity that left us a lot less hopeful than informed than the information you have provided for us today.

I want to begin by asking Mr. Adelson a question. Putting what you do in the perspective of first responders is very helpful. And communications, steps in information management, is an issue for all of the first responders, the fire, police, everyone. Is this a part of the ongoing dialogue that the private sector is having with the federal government? And do you have any recommendations as to what this committee can do to better make that more efficient so that you can respond in a timely manner?

Mr. ADELSON. Sure, I believe that there is a lot of learning going on right now, and I should stress that we are in the initial stages of determining where the threshold should be in information sharing. Information sharing being the critical component, as you have said, as an exchange point operators seen the communication problems that go on between network and service providers and vendors in government today, we know that it is a monumental task and should be approached very carefully.

Classic example of this is the Freedom of Information Act provisions that really must be preserved to protect network service providers so that they can freely share that information with government without concerns.

And I feel that that is one example of a number of areas where really we have to understand the full scope of what is at stake for network service provider before engaging in any kind of formal process.

But I am encouraged by the process that is happened so far on the standards and suggestions that I have seen.

Mrs. CHRISTENSEN. You raise the trusted environment again. And that is really critical between the private—between private industry and between private industry and government. Are there recommendations from any of the panelists as what this committee can do to foster that trusted environment so that the communications can flow as it needs to flow?

Mr. IANNA. The trusted environment can exist in a government-private partnership. We have seen it work in the telecommunications environment. We are concerned about sending lots of information to not only one place, but multiple places to then have it become public, which may not be in our best interests.

The other thing, I think, that is really important is to get to the level of protection that I think we all want. A macroanalysis of vulnerabilities will not get you there, in my opinion. You have to get to the microanalysis of each and every industry and network.

An example that I give is I could create a network for a large bank out of AT&T services, SBC services, Microsoft services, Equinix services, et cetera. And that could be very, very physically secure and very logically secure. I could take the same bank and the same four vendors and create a network that is not physically secure and not logically secure, just by putting the parts together differently or having absence of pieces.

So a macroanalysis does not get you there. It is a microanalysis, and it has to be done at the industry and at the entity level. A lot of the components to create very secure, cyber secure, and very physically secure networks are there already. And a macroanalysis of this may not get you there. It has to get down to the, I believe, the individual network level.

Mrs. CHRISTENSEN. Well, maybe I can—I don't see anyone else jumping to answer, so I will ask my last question.

The government and the private sector have been collaborating and discussing security before the creation of the Department of Homeland Security. Has there been good continuity in that collaboration? Has it improved? Has the creation of the department, bringing all of the different parts under one umbrella, has it become more cumbersome? Has this dialogue between the private sector and the government improved since the Department of Homeland Security over these issues? Or is it more complicated because of all of the different pieces coming under this one umbrella?

Mr. ADELSON. Well, I will say that my experiences before the Department of Homeland Security, while encouraging that there were efforts underway, we are, you know, minimally exposed to. Part of it is because, you know, we were focused on our customers and we didn't have the resources to have someone here in this environment at all times to interact with government.

One of the components of DHS which was encouraging for us was they were reaching out. And for the first time we were hearing from government with a request to learn. Like this hearing today is a great example of that. So I think we are headed in the right direction.

Mr. IANNA. I would just like to say that as part of this, many state governments have done something similar. And certainly, from a response request and the amount of effort that you have to put into it, and the vulnerability of information and create a few lists in 51 places, as opposed to one place, also. I would like to see more coordination and templating amongst the states to the federal level also. I think that would be very helpful.

Mrs. CHRISTENSEN. Thank you.

Thank you, Mr. Chairman.

Mr. THORNBERRY. Thank you.

Vice chairman of the subcommittee, Mr. Sessions?

Mr. SESSIONS. Thank you, Mr. Chairman.

I am sorry to have skipped back and forth, but I heard the testimony from Mr. Diffie, and I heard you talk about standards by the government. I heard, certainly, Mr. Ianna talk about government standards that would be good for us to development. And part of the dialogue and discussions then that Dr. Lowery was the CIS.

The question I have got for anyone on the panel is is there any consensus on a best practice?

Mr. Ianna, I just heard you say you could develop a secure network that would be great. And depending on how you put the pieces of the puzzle together, it may or may not be secure using even the same vendors.

Is there a best practices model out there that should be looked at, sanctioned, if not by some government entity, by I think they are called CIS? Is there something out there today that says this is the most secure way that we know of today to develop the architecture? Or would everything just be so robust you would have to literally pay somebody thousands of dollars to come and piece, part it for you? How difficult is that? And does the government follow a model, from what you can tell, as related to whatever this business model may be? Anybody?

Mr. IANNA. I will try a shot. There are best practices that industry participants have shared. The NRIC previously the NRC is a good example of that. As we came across failures and we analyzed failures, we figured out what do people do? And what do people do well and what do people do not so well, or companies within that? And we created best practices and we shared them. And we are doing that right now in NRIC 6 at the physical level and at the cyber level.

But to paint the entire problem, I believe, with one set of best practices, I would just urge that we don't fall into the trap. For example, a best practice for a financial application at a very high level transmitting, you know, hundreds of millions or billions of dollars in transactions may be one set of best practices.

And somebody surfing the Web for information may be a totally different set of best practices with different levels of security, fire walls, et cetera.

So I believe that best practices do exist in industries. I think we have some proof of it in the telecom industry. I can't speak for others. I think there are—power industry, for example, et cetera. But I don't know if there is one best practice that fits all sizes of all types of networks and applications that the government should sanction. I don't know if we should go that far.

Mr. SESSIONS. Then, what would you say? Dr. Lowery, you might want to speak to this, but what would you then say, and your observations about the United States government, following these known best practices, how well do you think they do?

Mr. IANNA. Well, that is a good point.

The government is a very big customer. And it can drive some very big changes in the industry or practices in the industry just from its own purchasing power. So if the government decided, for certain networks, that it wanted these levels of cybersecurity, firewalling, anti-virus software, automatic updates, et cetera, it could drive that particular standard for that level of security because you have the purchase power of a large customer.

Mr. SESSIONS. And how well do you think the government does?

Mr. IANNA. I really can't paint that with one brush. I don't have an answer.

Mr. SESSIONS. Good. There are examples of very, very good? Or do you enough about this to speak on this?

Mr. IANNA. I probably don't know enough about it.

Mr. SESSIONS. Okay. Thank you.

Ms. GAU. If I may, I just wanted to pick up on one element that Mr. Ianna mentioned. And that was the auto updating.

When you look at some of the organizations in the industry today that put out security standards, there are a number of them other than CIS. And they try to market it as a service. There are even security seal programs just like there are privacy seal programs where the industry is trying to take a self-regulatory approach to establishing a baseline level of security for certain applications.

The problem is that as we have already said, security is an ongoing process and a moving target. And as part of any of these standards, as part of any potential piece of legislation, it needs to be auto updating. And there lies the dilemma.

Mr. SESSIONS. I would love to see it stay away from legislation, but to be able to say there is some standards body that we believe enunciates the best practices and becomes a model. And somebody talked about this. I think that that could be a way to highlight someone. And I think that is the best way that we ought to pat somebody on the back but not with rules and regulations.

Dr. Lowery, did you have a comment or someone else?

Dr. LOWERY. Just wanted to expand on the Center for Internet Security and also what has already been said, just to expand on that somewhat, that security is not one-size-fits-all. There are best practices, though, which are broadly applicable. And the Center for Internet Security benchmark level one is intended to be that kind of best practice.

They also have level two benchmarks, which are much more rigorous. And then you could also turn to individual companies and the products that they provide, and they can give you also their recommendations on how to best secure their products. So you look at the situation in which the technology is going to be deployed. You adopt best practices, which everyone has already agreed these are good ideas, and then you specifically tailor the security for your environment.

Mr. DIFFIE. So let me speak to two aspects of what you have said. One is that the question you are asking about how well the government has done is really one in my mind that if in need of objective measurement, that is to say, I think, that it would behoove the government to just go through, make provision for assessing the security in operations of the computer systems its using.

And then, asking about each individual sort of product and installation configuration, should we have been doing this. Should we continue to buy more things of this kind from the spender, whatever? A reactive—an energetic, a due diligence customer approach.

The other point is it is the most critical thing in security in many ways, is a realistic vision of the threats. And we have before in Washington seen the impact of unrealistic visions in both directions, one of which is not to worry about it, and the other of which, particularly during the Cold War, is to let us security enthusiasts, and I have—though were many in the federal government, get in a position to try to push, in this case, civilian agencies to meet various kinds of military standards that merely cost a lot of money.

And because there was a general—not an inevitable, but a general antagonism between security and flexibility, you must be very careful about how you impose practices and security standards on agencies so as not to interfere with their getting of their work done, which is the primary thing.

Mr. REITINGER. Briefly, Congressman, to re-emphasize what Dr. Lowery said, there is no one-size-fits-all solution. Anyone taking a particular configuration of the system, for example, needs to take a look and see whether that meets their particular environment.

But one additional point, one thing that can be done, and something that Congress did last year was pass a management framework for information security in the federal government as a part of FISMA. So that is not a one-size-fits-all, that is actually a man-

agement framework that addresses security in federal government systems.

Mr. ADELSON. You asked a specific question about whether best practice could secure, and I just wanted to point out best practices are important, but there are still a lot of research that needs to be done at the industry level to fully secure vulnerabilities that we have exposed over the course of the next few years in the infrastructure, and we can't just leave that. Federal government could help with funding of research, for example, to help us get us there.

Mr. SESSIONS. I thank the panel.

Thank you, Chairman.

Mr. THORNBERRY. I thank the gentleman. And I might mention next week this subcommittee is having a hearing trying to focus on the research and development ahead and what those needs are and how those resources ought to be directed. And so, I think the gentleman makes a good point.

The gentlelady from California, Ms. Sanchez?

Ms. SANCHEZ. Thank you, Mr. Chairman. I have some specific questions for—and so, I will call out the names when I come to the question for you all.

I just want to say thanks for having me, Mr. Chairman, and I know I have learned quite a bit.

I am a member from California, and I represent Orange County, which has a pretty good information and high-tech community. So I have been working with some of my colleagues, like Anna Eshoo and Zoe Lofgren and others on some of these issues like encryption and everything over the years. But I mean, this is just such a large area for us to try to focus on. I really appreciate all of you being here today for it.

Mr. Reiting, even if an underlying operating system is considered secure, can programs running on that platform still cause problems like spreading viruses or attacking other systems? And if that is the case, would we need to security check every piece of software that we run?

And if we do that, do you foresee proprietary problems if its necessary to check source codes of all programs, for example, for security holes, embedded viruses and other issues?

Mr. REITINGER. Certainly, applications as well as operating systems can have vulnerabilities and can pose difficulties. I think what is essential is to use software that is developed by companies that use a robust quality assurance or software assurance process where they, in the course of development do—use trained developers, track their source code, do code reviews, do external third-party reviews, do penetration testing and seek external certification, such as the common criteria, for their products.

And I think that provides a fair amount of assurance that the products are as secure as they can be under the circumstances.

Ms. SANCHEZ. Thank you.

Mr. Diffie, you say that the latest encryption standard is as secure as you need to be. And I was just discussing with Ms. Lofgren where we were with encryption, because we have been working on this for awhile. I know it is a regulatory process now, and we seem to have an ability to move encryption standard, if you will. Can you

explain what you meant by as secure as we need to be at this point?

Mr. DIFFIE. I apologize—I don't think that was probably exactly the term I used. I think I said a secure as one could want. And what I meant precisely is that when the data encryption standard was fielded 25 years ago, it had to give, getting into technicalities, a 56-bit key, about a billion billion possible keys.

And that number was chosen, at the time, to be a compromise between the desires of the intelligence community and the perceived security needs of civilian government.

The advanced encryption standard offers three different key lengths: 128, 192 and 256. And as far as my community, the open cryptographic community can tell, and as far as we understand from NSA, what they believe, we do not know how to break into AES encryption at any of those key lengths faster than just looking through the keys. That is infeasible at all three of those lengths.

And so to take the words of the preface to an old Soviet encryption standard, this algorithm places no limitation on the security of the data to be protected.

So that is exactly what I meant, that the intent here and what we observe in the public community and what NSA tells us all accord in saying that this is as secure as any cryptographic algorithm we know of.

Ms. SANCHEZ. Thank you. I hadn't quite heard it put that way so thank you for your information on that.

Dr. Lowery, you talked about a partnership between the vendors and the customers. Vendors provide security-minded products, and customers make sure that they have proper security settings. I am concerned about the customer who might not know how to keep things secure or inadvertently creates problems within the system. Can you elaborate on the responsibilities that you think we would like to see customers take on with respect to security?

And how do we, as a government, encourage that? Because, you know, we are as secure as our weakest link and it could be one of these users.

Dr. LOWERY. I think one of the most important things you can do is to educate end users, not about technical aspects of security, but simply about the role that they play as individuals, as gatekeepers, into a larger community of data sharing and information sharing.

If we could get the end users to understand that as a participant in e-mail, for example, simply opening an attachment has ramifications that not only affects them, but could affect others. Just an awareness of their ability to impact others through how they use these technologies could go a long way to improving security for everyone who participates in these systems.

Ms. SANCHEZ. Thank you.

I see that my time is up. I have some other questions, but I will submit them for the record, Mr. Chairman.

Thank you, gentlemen and—

Mr. THORNBERRY. The Chair thanks the gentlelady.

The gentlelady from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman. And thank you and the ranking member for holding this important hearing.

To the panelists, thank you for your presentation and your indulgence on members who have several hearings going on at once.

Let me take personal privilege and express my appreciation that Dell is still in Texas, in Austin, Texas. We are gratified for that. And to thank AOL Time Warner for being one of the first groups to host members of Congress out into the Virginia location. I think that is prior to the merger, but we thank you very much. This is an important issue.

The bell is ringing, I believe, so let me quickly comment.

Mr. THORNBERRY. If the gentlelady would yield briefly?

The Chair's intention is to go until we have about 7 or 8 minutes left in this vote. My understanding is we have two votes. And then I would like to come back. Hopefully, we would be gone no more than 15 minutes, and then we could resume. And so that is my intention.

Thank the gentlelady.

Ms. JACKSON LEE. In an article, and the date is a little fuzzy, so I will just refer to the article, talks about the administration abolishing the high-level Critical Infrastructure Protection Board and the fuzziness of the administration's position on cybersecurity. And I would be interesting in your assessment on what the sense of the industry is with respect to where government is on cybersecurity particularly in the loss of Richard Clarke, who was a very visible government person on these issues and the fact that this board now has been recomprised in DHS with a lot lower profile and staffing, if you are familiar with that particular board.

But that was the board that had the face of the administration, and that is the Critical Infrastructure Protection Board that generated after the turn of the century and of course, after 9/11.

My question is what can we do in government as relates to cybersecurity? And I ask these questions. Do we need more information sharing? Do we need more firewalling? And do we need a best practices? And in your opinion, what are the three things that the government may need to do immediately to improve cybersecurity? If you want to point it at the department or point it at this select committee because we are supposed to be the fixer-up-it in terms of trying to find solutions.

I would appreciate your response to that, whoever wants to jump in. Or we could start—we will start in that direction, yes.

Ms. GAU. Thank you. I appreciate you reference to the former Critical Infrastructure Protection Board and Richard Clarke, whom I worked with quite closely, with him and his staff on the national strategy that came out. One of the things I have noticed is that there has been little reference, other than my own, to the national strategy to secure cyberspace. And although there are critics of the document that say it is too watered down and that it does not really lay out responsibilities, it simply makes recommendations.

It nonetheless serves as a blueprint. And there are detailed actions and recommendations outlined in that document that address all of the issues we have been discussing today.

One of my recommendations would be to indeed look at that document, engage more actively in pursuing the actions and recommendations in the document, and to look towards perhaps elevating the level of attention that the national cybersecurity division has right now.

My personal experience and AOL's experience has been that when that board existed and Richard Clarke was in place, we had a much more active relationship with the White House on cybersecurity than we do now.

And whether or not the placement of the national cybersecurity division within DHS is the appropriate location is not something that I believe I am qualified to speak to. But we would like to see a similar level of attention and priority given to the issue of cybersecurity.

Ms. JACKSON LEE. One of the points you mentioned was firewalling versus information sharing. And let me just say that security is an almost unlimited excuse for keeping things secret. And very often in the short run that is the right thing to do. But I think it should be recognized that secrecy in regard to security matters should always be thought of as a vulnerability. Because no matter how hard you are trying to keep a secret, your opponents might discover it. And the ideal security systems are ones that operate in a very open environment, and do not depend on secrecy about themselves.

So I want to say that although we in industry very often have a parochial interest in the government helping us keep secrets about how our products work, about what our vulnerabilities have been, that the long-run interest of government is probably in promoting and requiring greater openness.

Ms. JACKSON LEE. Can I get one person to answer the question, what the government needs to do right now in cybersecurity—just one person, and then?

Mr. ADELSON. I will say—

Ms. JACKSON LEE. I appreciate it.

Mr. ADELSON. —promote the Department of Homeland Security as the epicenter of information sharing for industry and federal, state and local government—number one.

Number two, preserve the federal information act protections and the Critical Infrastructure Information Act.

Number three, consider funding for outreach to promote the sharing, research and development of security and testing.

I just want to say that that is an introduction. Right? But that is the immediate thing that could see support for, those three things would be critical right now.

Ms. JACKSON LEE. Anyone else?

Mr. IANNA. Just to echo that, there are some examples of ISACs that I believe are working well. I could speak for mine in telecommunications industry ISAC as well as the Network Reliability Council sponsored by the FCC. We see effective partnerships between the government and the private sector, particularly where the government is funding part of the infrastructure, which I believe is important, which the other ISACs may not be experiencing. That might be a good model to move to those other ISACs.

Ms. JACKSON LEE. You think it needs to be elevated in the Department of Homeland Security from where it is now?

Mr. IANNA. I can't say that. I just say that there is an effective—it seems to be, from my perspective in this industry, an effective model in Homeland Security right now, in telecom ISAC.

If the other ISACs are struggling—and I don't know if they are—with information sharing, maybe a funding, a government funding of some of those ISACs would be helpful.

Ms. JACKSON LEE. Does anyone believe it should be elevated from where it is in the Department of Homeland Security to a higher presence, this whole idea of cybersecurity?

Mr. DIFFIE. I am willing to say yes, but I think that is something to give a considered answer would require a bit of study of what is actually being done, organization of the department.

Ms. JACKSON LEE. Did you have a response, sir?

Mr. REITINGER. I would say that I think cybersecurity is a critical issue. I think one reaches a point where reorganizations become harmful rather than helpful.

What we are interested now is seeing action and working with the department to make it as productive and effective as possible.

Ms. JACKSON LEE. Thank you.

Mr. THORNBERRY. The Chair thanks the gentlelady.

As I mentioned, we have two votes, and my intention is to be back in about 15 minutes to continue this hearing.

Again, I thank all of our witnesses for their patience.

And we will resume shortly.

The subcommittee stands in recess.

[Recess.]

Mr. THORNBERRY. The subcommittee will resume its setting. Obviously, other members are going to be coming back after the vote.

And again, I thank the witnesses for their patience.

Let me ask about a couple of areas as members are coming back. One of the things that I am struck by in each of your testimony today is a somewhat different tone from some of the testimony we received before.

In some of our previous meetings and hearings, there is a feeling that the advantage lies with the cyber attacker, that the advances in technology are really working to the advantage of the people who are trying to break into systems and find out things, and that our response is lagging further and further behind, and for a variety of reasons, which they have enumerated. And it is a somewhat pessimistic view of our country's ability to protect against particularly sophisticated sorts of attacks.

I would be interested in that larger sense from what you all see in your business dealings every day, whether you share that view of and concern that attacks are growing exponentially both in number and in sophistication. And that it is going to be very difficult for us to stay ahead of the bad guys, if you will.

Mr. Diffie?

Mr. DIFFIE. Well, let me suggest to start with that we are ahead. Our economy, I know, is not as its best at this instant, but fundamentally, it is a great, thriving, robust institution. Our society, likewise. So a lot of the way you view this issue of how many attacks there are how sophisticated they are, how much damage they

did you is really just a matter of setting thresholds, which are going to come out very emotional, because loosely speaking, any level of attack is irritating to us.

And I would be very skeptical that on balance development and cyber attacks so far could actually be said to have slowed our society down very much.

Moving to a slightly more technical level, I would say that we have unquestionably made major achievements in some areas of security, which, if adequately widely deployed, would put an end to many of these things. And so, this again comes down almost to a matter of definition. When you are trying to protect, you are trying to protect the whole curtain wall of your fortress. And somebody who punches any hole through it gets credit. So we will probably always be chafing at the number of cases in which we failed.

But I think that if you look at the overall development, and not just of security techniques, but of computer software. You will find it is far more robust, far more reliable, far more resistant to attack today fundamentally than it used to be.

The difficulty comes out of the degree to which this is a dual-use technology. And the technology is in the hands of a wide diversity of people, some of whom don't have our best interests at heart. What worries me maybe most in planning about this is that we think of it a lot as cyber crime and as a cyber nuisance.

And that as so far, we have not seen any 9/11-like, let alone a nuclear bombing-like attack on the United States by cyber methods.

I believe it is still a matter of speculation whether that could by itself be comparable in damage. When you look at our own military doctrine, we use cyber warfare conjoined with physical warfare.

But the thing that worries me is that we are not making sufficient preparation for protecting ourselves against cyber attack by what I think of as real enemies, enemies who have assets outside the United States, outside the control and to some degree outside the retribution of the United States, who can develop and cook their attacks long enough that they will be really dangerous when they happen.

Mr. REITINGER. I would just reiterate, Mr. Chairman, that I am equally positive about what industry can and will accomplish. I think the priority has changed.

One area that we do have to attack is the issue that has come up a number of times of information sharing. Sadly, hackers are still better at sharing information than perhaps we in government and industry are. They are great at describing vulnerabilities in systems and building wonderful GUI-based attack tools to use. We need to share information to that same level.

But I remain very positive that government and industry working together and industry innovating will achieve new and better security solutions. And we are actually better off and we are getting better off over time.

Dr. LOWERY. Mr. Chairman, I would add to that that a pessimistic or defeatist attitude is not warranted. We have a very positive outlook on this as well. There are really no technical reasons that we should be less secure than we are perceived to be.

Again, I point back to education as a prime component of this. That many of the problems that continue to arise, this lag that you may be perceiving is really a gap in education, which we could rectify if we put resources behind educating those who are using the technology so they use it in a more responsible manner.

Mr. THORNBERRY. And Ms. Gau?

Ms. GAU. With respect to AOL suffering a debilitating cyber-attack, I would be optimistic in saying that I don't believe it could happen. However, let me just say that AOL is attacked by hackers on a daily basis. We see all forms, all varieties and all numbers of hacker attacks. And they have increased and varied in techniques over the years. And as a result, not only have we had to invest money into the systems that we have in place to monitor the network, but also the staff that we have in place to be there. We have also had to make sure that we are eternally vigilant about these issues.

And to the extent that we remain vigilant and that we use the security technology that is available today, I believe we are in a good position. However, there is still the human element. The human element being the weakest link. And there, again to reiterate education, it is not only on a public awareness level, but it is also making sure employees are trained, that they understand what are the steps that they need to take.

Mr. THORNBERRY. And I want pursue the education issue in just a second. Just real briefly, are you finding it more difficult to stay ahead of the hackers? I mean, you said you are putting more resources into it, is it becoming increasingly difficult to stay a step or two ahead?

Ms. GAU. I would not characterize it as being more difficult, no.

Mr. THORNBERRY. Okay, that is helpful.

Gentleman from New Jersey, Mr. Andrews?

Mr. ANDREWS. Thank you.

I would like to thank the witnesses for their outstanding work and testimony today.

Thank the chairman and the ranking member for another in a series of truly edifying and challenging hearings. Thank you for your work.

I want to go back to the question the chairman raised at the beginning of the questions here because I think it is the central focus that we have. He asked whether the panel thought that the market alone would bring us to a sufficient point of security or whether there was a point beyond that. And I think I heard the consensus was that although the market would take us a very long way indeed that there was an increment of security above and beyond what the market would do.

The second point of consensus that I am hearing is that one of the ways, one of the most effective ways the government can help us stretch the market, stretch the market solutions is through the creative use of our purchasing power as a customer that demands these products.

The third thing that I am hearing a point of consensus is that that purchasing power must be carefully calibrated and distinguished among various sectors. What the Agriculture Department would buy would be something very different than what the De-

fense Department would buy. That it needs to be continuously upgraded. A theme that I am hearing from the panel, and really from the members, is that if we have a static standard of what is sufficient that you are all going to leave us behind in the dust, at least I hope you will if that is the case.

And the final point of consensus that I am hearing is that—I think I am hearing is that we need to do a surgical and thoughtful job of articulating what those standards ought to be. We shouldn't haphazardly define the standards.

What I would like to ask the panel is if I have misstated any point of consensus here, please tell me. And I say that without pride of authorship, I am simply reporting what I think I hear, number one. And number two, if it was your job to design the standard-setting function within the Department of Homeland Security and within the U.S. government generally, what would that institution look like? What kind of institution would it be that would tell our purchasing people what it is they should demand when they buy a system that protects the Social Security Administration's record? Or when they buy a system that protects the troop deployment databases of the Marines Corps? Or whatever else.

And we will start with our friend from AOL at the right side.

I, just parenthetically, my last name begins with 'A' and in law school a lot of professors call on students in alphabetical order. It is a very harrowing experience. So when I taught law school, I start at the other end of the alphabet so I wanted the people at the other end to get their just deserts. So because you have had to wait so often today, we will start at your end.

Ms. GAU. Picking the latter part of your question with respect to what would an institution look like that might set security standards for the government, I think that the model of everything we are talking about where it would be an institution that would work closely with the private sector together, as we all hope to do, with Department of Homeland Security. That there would have to be dialogue to establish what the baseline security standards would be.

And such an institution, presumably, would have tentacles into procurement processes such that they could mandate the different standards, just as there are other standards such as those that I have referenced earlier today such as accessibility standards and products.

Where it might best fit, I don't think I am really in a position to say either. But I think that such an attempt by the government to indeed mandate that as a customer and a consumer of these goods that government would move in the direction to push manufacturers and service providers to include the baseline security standards is a step in the right direction.

Mr. ANDREWS. I want to be clear also, as I know you said, I am not talking about mandating standards on the private sector. I am talking about mandating our own internal standards for demanding product when we go into the private sector.

Yes, sir.

Mr. IANNA. I think the question has to be answered this way, what level of security do you want to be able to espouse? Do you have a metric to be able to easily convey to the public that we have

raised the cyber-security level to this level? And we have to create that metric, just like we had to create the metric in network reliability.

What are we talking about? We are talking about, you know, how many DPMs, defects per millions of failures you have and what constitutes a failure, et cetera.

And then I think it has to be done on a—you can't eat this elephant all in one bite. You have to do it in small bites. And every sector needs to define, I believe, their critical systems that they need to have cyber-defense around. And once you have done that, do we have, for example, the critical systems cyber-protected to this gold level in the Department of Agriculture or how long will it take us to get there.

Then I think—if I were in the government, I would be trying to convey to people that we have a methodical way of convincing people that we know what we are doing. We know what direction we are going in. And we know how we are on our journey to get there.

And secondly, lastly actually, it is not static. The minute somebody says I am protected to the gold level, a new threat comes in and the gold standard has to be redefined.

Mr. ANDREWS. Sir?

Mr. ADELSON. I believe that that is the key is the dynamic nature. And perhaps one way to achieve a dynamic standard, if you—that is kind of a contradiction in terms, but—is to actually involve in real time, industry. And by real time, I mean having individuals who represent industry be part of a panel wherever this group sits in government, where they can provide that data and how it has changed in real time.

And I suggest that just because industry, because of the market forces, is going to be thinking about that with a great degree of diligence. And I would expect that their message should be heeded, even across different sectors, as it applies to, you know, buying power within government.

Mr. ANDREWS. I hear you. Boy, that would raise significant issues about protection of intellectual property. I mean, we want to do that, but we want to do it in a way that doesn't punish the private sector concern for participating in that, right?

Mr. ADELSON. I think there are certainly protections that can be put in place so that communication can happen. I can tell you that it is relatively rare, although it does occur, where, you know, data about an incident is something that I might fear being propagated.

However, data about the security technology itself is really mostly, in terms of consumer products, you know, certainly the case, public data. And there is a lot out there which would go a long way. And certainly within the standards set, I would hope that these would be technologies that everyone can purchase.

So there isn't a lot there to hide.

Mr. ANDREWS. Thank you.

Dr. LOWERY. Congressman, I think you have accurately summarized at least what we believe at Dell. And as far as how I would structure this entity that you have referenced, I don't know that I would be an expert in helping you to architect such an organization. But things that you should consider when you are developing the standards for the government, consider what I said earlier and

that is that there is a baseline of security which is just prudent for everyone to adhere to. And then each particular application of technology must be scrutinized in the context in which it will be used and security for that purpose needs to be customized for it accordingly.

Mr. ANDREWS. Thank you.  
Sir?

Mr. DIFFIE. I think that what we have to keep in mind is the breadth of the activity you are talking about. Government has a major movement in the last, say 20 years, to move to commercial off-the-shelf technology to support all its activities wherever it can, to narrow back the, you know, technical nuclear, the technical comsat with things. It all stems from going away with the national arsenal system 80 years ago.

Second, all of this is in some sense dual-use technology in terms of the role it plays in cyber-crime and cyber-warfare and cyber-security. So you are building things out of standard components, components that people use for a very wide range of things in society.

And finally, this is an international problem. We cannot afford, as we did during the Cold War, to think of our own security needs in isolation from those of our trading partners and indeed the rest of the world.

So let me suggest that this organization, which is going to need to walk down the Potomac on its tiptoes, I am afraid, has to be a meeting ground with a prudent ability to manage information relations between quite a number of constituents. Its government customer—and I construe that broadly; the intelligence and law enforcement communities on which it will depend for a lot of the kinds of feedback information I have been talking about; the industry on which it will depend almost entirely for products and processes and support; and the international community, the international standards organizations and many different kinds of governmental and non-governmental and industrial organizations throughout the world.

So the best I can say is I am very in favor of openness in the standard-setting function. And that that should be specialized so the cases where closed things are needed, that we should give careful thought to the way the information-restricted activities take place and be sure that that is subordinate to the general openness that will allow us to accommodate ourselves to everybody's needs.

Mr. ANDREWS. Follows your principle that secrecy creates vulnerability as I think you said at the beginning.

Mr. DIFFIE. Yes, actually, I think that actually this principle's a little broader than this. My view is this is infeasible without a lot of information-sharing that has been stifled in the past.

Mr. ANDREWS. Yes, sir, thank you.

Mr. REITINGER. I will be very brief, Congressman. First off, on standards, one suggestion I would have is that as, again, I am repeating a lot of what Whit is saying, that we avoid having specific government standards to the extent possible. I think if you rely on industry-based market-driven standards, you will find the government keeps more up to date than if it sets government-specific standards which will maybe become hoary in a shorter period of time.

The second thing is that I think it would be useful to turn and see what is happening at NIST under some of the processes started under the Federal Information Security Management Act. NIST—I would have to go back and reread the act, but I know NIST recently published FIPS 199, which has a categorization of information and information systems into risk categories.

My understanding is that under that last act, they are going to go on and produce guidelines for how to protect that information. And that might be a very valuable process for this committee to look at and watch.

Mr. ANDREWS. Thank you very much.

Thank you, Mr. Chairman.

Mr. THORNBERRY. Thank the gentleman for, again, asking excellent questions.

The ranking member of the full committee, the gentleman from Texas.

Mr. TURNER. Thank you, Mr. Chairman.

First, I want to compliment you, Mr. Chairman and Ms. Lofgren, our ranking member, on your leadership in the area of cybersecurity. Those who have been a part of your hearings and your also compliment you on the leadership you are both providing in this important area.

Dr. Lowery I want to compliment Dell for your leadership in providing or offering your Center of Internet Security Level I benchmark to your customers.

There is no question that your business model selling directly to customers provides an excellent opportunity to promote the purchase of a secure computer system.

I guess your interest in providing security arose out of the Department of Defense requirements. By then turning that into an offering to others with the stamp of approval of the Center for Internet Security, it seems to me that it should become something very quickly that most people would want to pay for.

Dr. LOWERY. We agree with that assessment too, Congressman. We were directed to CIS by federal customers, who pointed to the CIS as a source of best practices that they agreed with.

We evaluated the CIS and their benchmark settings, and we heard that a product offering where we could make those settings in the factory was feasible, that we could do as our customer requested. We did that, and we got it in such a way that others can benefit from our work and the work of CIS.

We are very excited about the offering. We hope that it will contribute to improving the security landscape as it exists.

Mr. TURNER. Well, I commend you for it. The issue before us and the same one raised by Congressman Andrews: How do we replicate this? As I understand it, there is a host of entities out there that say they certify or they recommend certain security measures. Every company, you know, is looking for somebody. Not everybody looks to the Center for Internet Security. Some look to other groups out there.

If we want to accomplish what I think is the goal that most of us share—self regulation—we want to be sure the industry provides the leadership on security initiatives.

As has been pointed out, if government is the role of creating standards they will be outdated the moment that they are drafted.

It is clear we need a viable ongoing effort among industry partners to set some standards.

How would you suggest, Dr. Lowery, or any of the witnesses, that we decide on a consensus organization made up of that we would look to as the good housekeeping seal of approval, if you will, for security. We should have something so we would know that if it had that stamp of approval on it, then that was the best you could buy. As you all have said, if you don't want to buy such a certified approved product then that is your choice.

At the very least we would have provided an industry-wide approved certification that is recognized by the buying public. Then we would encourage the buying public to make a choice. The reason I believe strongly that is the right way to go is I think security is on everybody's mind. I think this problem can be solved in this fashion voluntarily, if industry will work in cooperation with government we will have a standard-setting entity that everybody knows about and respects, and therefore, will follow.

I know how it was in our house when we made our last computer purchase. We were thinking about security now. And I think most people are. I don't think any business in America wants to be caught short in not providing security to its business systems.

The liability and the risk are too great.

So how can we get there with a standard that people will follow?

Dr. LOWERY. I think everything you said is true. And I also perceive that there are a lot of little organizations, for lack of larger ones. Each of them are trying to make sense out of the security problem and have delivered into the spaces they perceive where there is a gap, what they call their standard or a consensus that they have arrived at.

I think all of them are valuable. None of them should be belittled because their stuff often comes from small sector doing something.

But I do also see the need for convergence, a consensus process. Dell would also welcome seeing a more consolidated approach to achieving the standards. The fewer standards that there are, the easier it is for us to bring them to market.

The only caution that I would give you in trying to approach a singular standard or a single organization, which does that, is that organization must understand that security is not one size fits all. We had to be very careful in its deliberations and in standards that it might recommend. To keep that in mind, that we must be sure that security fits the situation, that it is going to be the deployable technology.

As far as the way to actually achieve the convergence, I think we are seeing some of that already. I am not exactly sure what to recommend what we do to hasten the convergence.

Mr. TURNER. Anyone else?

Mr. DIFFIE. Let me extend that not one but sole point as saying it is important to remember that security is always a secondary objective. You always want to do something and you want to do it securely. So having an underwriters lab like stamps that would go on everything happens to be particularly tricky in security, because security is more contextual probably more than the other safety

technologies. And so although your car, of course, depends on how it is driven and how it is maintained, as well as how it was built, that kind of environmental characteristics are even more important in the security area.

So I think that a labeling scheme, we already have several, is not going to be trivial to achieve.

Mr. REITINGER. Two brief points, Congressman. First off, as you suggested, there are lots of good standards or other organizations out there developing things and certifying things such as the common criteria.

Second, I have got some very good news, which is although one size does not fit all—I agree very much with that—it is important to have as much consistency as possible among different people providing advice to consumers.

And so Microsoft, for example, is working closely with the Center for Internet Security to converge our guidance on how to secure our products going forward. That kind of activity is taking place in industry. We are talking amongst ourselves and we are trying to solve the problem. And I think we are solving the problem.

Mr. TURNER. Thank you. Thank you, Mr. Chairman.

Mr. THORNBERRY. Let me delve—I thank the ranking member—let me ask briefly about the information sharing, because a number—we have talked about it a lot and it has come up in different contexts. Mr. Ianna, you talked, I know, specifically about the telecom ISAC and it being successful. What I hear from others is that their ISACs are not nearly as successful as you have become. And you mentioned government funding being one of the things that is not the case with the others.

And then I am also struck, Mr. Adelson, one of the comments you made is that we share information real well on a technical level, but what that leads me to think, Okay, where do we not share information real well? That is going to be for the areas that are competitive, the things that are not so technical. And so the view has been expressed that there is a limit to how far information sharing is ever going to reach.

That when you are dealing with competitors and industry grouping, they are only going to go so far. And they will talk about FOIA, and then they will talk about anti-trust and then they will do something else that they talk about.

Whatever it is, it is going to be an obstacle to—and I am not criticizing that, but it is a natural thing.

I guess I am interested in observations—Mr. Ianna, I will start with you—about this subject of information sharing. Are there legitimate barriers that the federal government needs to break down? Or is it more a question of a trusting sort of relationship that has to develop over time, at least for industry to share information with the federal government?

So you see ISACs as—I will say salvageable—some people say they are not, need to start from scratch. And if so, how do we make them? And I realize there are too many things to get into. But I would appreciate each of your suggestions on this information sharing idea.

Mr. IANNA. Well, first of all, I think one of the other keys on the telecom ISAC and other structures surrounding that—I mention

ENRIC—is beware their time. They have been in existence for quite some time. ENRIC goes back almost 11 years. I don't know when. Probably more than that. So there has been time when they worked together.

Believe me, the first few years when we started ENRIC at NRC, we had the exact same thing. I can imagine that Microsoft and MCI and AT&T and Sprint saying we are all going to share our failures. All right, it was not easy, okay, number one. Number two, it came down to a situation that we realized that by very nature we were all interconnected. And we were all just interconnected. And the failures that we would see in one network might show up in another network because we all used similar types of equipment.

And I think some of those—some of those—you know, we all use equipment from a set of vendors that might experience a failure. So want to be able to know what happened.

And then I think that the next thing that we experienced was nobody likes to advertise a failure. And there was a lot of debate about, Well, when I have a failure, it is AT&T and can I ask AT&T?

And we had this debate. And we started out as they were masking it. And finally, after a while, we just said, Okay, here they are, here are the failures. And last year AT&T had 20-something FCC reports on this—had three. I know how many MCI had. I know how many Sprint had.

But the good news of that, the good news of that is that we do have quarters, 40 quarters worth of statistically valid data on failures on wire line networks. Now the debate going on at the NRC is others saying, Look, wireless for data networks, et cetera, will be voluntary. We will map the data, et cetera.

So I think there are ways of sharing the information. And I think what it all comes down to in the end is that we can improve the situation of the whole lot. There are competitive issues. We worried about anti-trust. We worried about information sharing and competitive things. And we had lawyers praying over that for a while. And we got past that.

And I think the end result has been that we have listed—now the FCC has sat in front of you, and you ask is the network reliable? Can it give you a number? Can you say it is getting better or worse? And they can break it down by quarter. And they can break it down by technology.

So I think the answer is it does work. It takes time. It takes trust. And the other issue of information sharing that I know a lot of people—and I am worried about also is when we do share information, is the problem about sharing information from one competitive entity to another, which you don't want to have happen as a competitive concern, but then making that information then public.

I think some of the protections that went into the Homeland Security Act around information protection are good and need to be enforced so that we don't have information getting pulled out under Freedom of Information Act, something that we have shared that we don't want to become public and also that doesn't become public.

Mr. ADELSON. There are a few points that we made that I would like to comment on. First, regarding the telecom ISAC, I absolutely agree that the telecom ISAC has worked for telecommunication-specific issues. But just using 9/11 as an example, during that crisis, there were between 25 and 50 extremely large critical networks and service providers in the United States who did not get any contact and were not part of any telecom ISAC. That is one issue.

Secondly, on recent research you could do on the Internet would point to over 13,000 independent entities that are relevant to Internet stability, even for the biggest carriers.

To put an ISAC together for Internet infrastructure would require representation not only from network service providers anymore, but from content providers, enterprise and vendors. Why so diverse? It is a function of the hierarchy used to be a carrier sold to a content provider who provided services for a user and so on.

Now it is much more of a level playing field. And those players need to be represented at a security level in discussing these issues. So I don't know how to do that with an ISAC with the Internet. That is one issue.

Secondly, you mentioned the technical communication that is going on. The real difference between the Internet and other industry areas where that communication happens is that the Internet is extremely interdependent. My ability to stay up is dependent on my peer—is the term used—and their ability to stay up. And so, because of that interdependency, there has been a tendency to communicate.

Furthermore, because security issues on the Internet are technical in nature, we have been fortunate in that most of the communication that is been required at least for disaster recovery are handled by technical people. I mean, there are exceptions, the provisioning side, for example, who somewhat separate from the technical. But there has been some industry success there.

And I think as we expand beyond network to network communications and go into network and enterprise communications, this is where I see a central point of contact, a central group becoming really critical, 13,000, 50,000, however many entities require some critical information. I am not comfortable relying on the industry itself to provide that intercommunication well.

Ms. GAU. Actually, you took one of the points I wanted to touch upon relating to information sharing and is there a competitive barrier to doing so. I think, once again here, we see the marketplace forces in action. As we are networks connected to networks connected to each other, and we are in the interdependent, even though we have points of redundancy.

If AOL sees a hacker attack coming on, that we might be able to sustain, but we might know that somebody else might not be able to or in more, should we say, self-centered interests, we don't want anything bad to happen to anybody else because if they go down, we are going to get a ton of mail thrown back at us from their servers as an example of a denial of service attack back on us.

So we are actually motivated not only to maintain the stability of the Internet and the ability of people, for example, to send e-mail to AOL, but also for us to be able to maintain our own service

and not have to then deal with a situation where somebody else has gone down.

Additionally, in that same regard, not only are we reaching out to individual providers and companies and partners that we have that we know are going to potentially be impacted by a particular attack or a particular vulnerability, we do share that information with government and we do so in an effort to ensure that that information is made available to the mom and pop ISP that may not be able to have access to that information because, as you have pointed out, they don't have the resources to have somebody sitting here at the table.

That is where we would really strongly like to continue to work with the government, in particular, the Department of Homeland Security and the new cybersecurity division.

Mr. THORNBERRY. Mr. Ianna, let me ask you one brief question. You mentioned, which is not something I had thought of much before the demands placed upon you from 50 different states for information, which is information sharing in a little different way. Do you think that there needs to be some—you mentioned a template which implies that the federal government would require certain information and the same sort of thing could be sent to the states.

Do you think that there is a need for some sort of legislation that preempts states from asking for the same or additional information? You know, we did that with ARISA on insurance where the federal standard is the thing that, you know, trumps everything else. If you are—if all of you could get demands from lots of different jurisdictions which would be impossible to keep up with, it seems to me.

Mr. IANNA. I don't—I can't speak to whether legislation at the federal level would be the best way to do it. I would say certainly, cooperation, or saying look, if we are going to have a standard, let us make the federal government the standard. And if I just need to parse out the data for this state, here is the data for that state.

I don't know. I could go back and research, but after the FCC at the federal level in NRIC, or NRC, started asking for outage reports, several states followed with that. I don't know how many. I think it is probably more than a dozen or so about outages in their states and whether or not they followed the same rules, et cetera.

But I think it would benefit the industry, only because of this—particularly in cyber defense, it is very hard to determine the geography of where the issue is and where it started. It might be impacting something in a particular state, but the cause might have been in a totally different state.

So trying to define geographic boundaries in a cyber environment is not the same as trying to define physical boundaries against physical attacks.

So from a cyber perspective, it certainly would be helpful to have a template or a focusing organization, like Department of Homeland Security, say let us do it this way. Let us do it once. And then we could give you your data, okay, that is, you know, for your state.

Mr. THORNBERRY. I suspect in all areas of information sharing that differences between industries are a key thing. I mean, I can see a number of the things you all are talking about that require

information sharing for the IT sector may not apply to electricity or agriculture, some of the other critical infrastructures which have been identified and may be the same case here. Depends on how much the states regulate, for example, electricity or telecommunications as to the leverage they have to put demands upon you for any information.

Mr. IANNA. Just one other point that was made by the gentleman to my right about the telcom ISAC and the IT-ISAC. One of the things that we found out is because, particularly on data communications and computer-based Internet communications et cetera, the telcom ISAC and the information technology computer ISAC are twisted together very tightly.

For example, with the slammer virus, our security people were not only working with the telcom ISAC, but also obviously with the IT-ISAC. It was the computers on the network that were causing the problem with the virus and that was impacting the networks. So they are very tightly twisted together. And you can't just look at one, they are very tightly twisted together.

Mr. THORNBERRY. Good point.

The gentlelady from California have additional questions?

Ms. LOFGREN. Just one. And I am mindful that you have been here a long time, and we certainly do appreciate it. I think really the information you have provided us, each of you today, has been enormously helpful. And we may want to follow up with you as we proceed with additional questions and ideas.

But listening today, obviously, this is a complicated area. But it may be further complicated by constraints that are being—that we may face as we go down the road. I heard the comment relative to the lawyers praying over the anti-trust implications. That was a cute way to put it.

Recently, we expanded the exemptions for anti-trust risk for entities that are setting open technical standards. And I think it is important that the openness be part of it. And I am wondering—this will be two questions—whether we have sufficiently addressed anti-trust concerns in the development of open standard setting in this arena?

And then secondarily, I can't remember who, mentioned the issue of the need to be able to deploy solutions in ways that are not burdened by intellectual property protection and whether anyone has advice for us in that area as well, those two implications of IP as well as anti-trust.

Do we need to change the law in any way?

Mr. DIFFIE. Well, I am not sure. I think there are ramifications from the question I don't understand. But the intellectual property issue has come in here in two different ways. One is a fairly ordinary issue of things that are particularly—are patentable and therefore royalties are owing to the patent holders in turn for using that technology.

The other is in this argument in the computer industry between open source and closed source coding practices. And that is one of the ones that I think presents a thorny problem because in security there is, as I said earlier, a very explicit respect in which closeness is a vulnerability. At the same time, proprietary techniques, trade

secrets are an essential basis of our business practices in this country.

So we need to find a business model that permits the users of products with security requirements and security implications to be able to verify that the products have the security characteristics they need. And to do this, to see if we can do this and still allow ourselves the benefits of allowing some manufacturers with proprietary techniques.

I don't have a clearer statement of it than that. But I believe it actually is one of the research frontiers in this area and it is a business frontier.

Ms. LOFGREN. One of the—I mentioned to Chris Henkin a comment that—I won't mention the fellow's name, and I don't think there is a chance in the world that the federal government will do this, that it was recommended by the—someone in law enforcement that we establish a kind of a software clearinghouse and that the federal government would clear, you know, all the software. I think that is a very bad idea.

But the issue is how do we achieve assurance? Obviously, not with a government agency. But how do we do this, for lack of a better word, the audit function for the security? Whether it is software or networks or hardware, how is that best achieved? How do we set up a structure so that occurs?

Mr. REITINGER. Congresswoman, I think my answer to that would be the one I gave when you asked a similar question earlier, which is making sure that the vendor that is providing the software has a robust software assurance and quality assurance process that the government can review and make a judgment upon. I think vendors are moving in that direction. A lot of them are there already. And I think it is important and valued for customers to know about that process.

Mr. DIFFIE. So I would say in this respect we should look at the successes and failures of an existing model, which is that for decades the National Security has been the executive agent for information security for the Defense Department and some other areas of the U.S. government. And they have done, in many ways, a good job.

On the other hand, the mechanisms they have, whose strength is in the, unfortunately, their unification of intelligence and security and their ability to trade off between the two and make use of their intelligence function in monitoring the security of their products.

They show no sign of being able to cope with the problem that we face, for the following reason. The Defense Department is a very large organization, but it is very unified. Everyone in the Defense Department knows the chain of command, starting with the President down through the secretary of defense.

And the important point about the Internet as a place is that so many people stand their by rights. You don't get to vet your personnel in the whole world.

So we have an extraordinary diversity. And I think your suggestion is one of the major critical points. You can ask what the track record and what the development methodologies of your suppliers are. It is also true that there is an ever developing methodology in

two directions. One is vetting individual applications, knowing that you are going to be able to minimize the damage they can do you.

This, just incidentally, is one of the targets to which Java is devoted. The other is in building operating systems that have sufficient capacity to confine applications so that the applications can't do damage to other things.

And this is one: The declining cost of hardware has allowed us to devote more and more hardware to that explicit objective. Sun's largest servers now have what is called hardware domaining, which is a very robust way of containing processes.

So I think that the proposal that the federal government should vet all the software is on the face of it is infeasible whether or not?

Ms. LOFGREN. Well, it is a non-starter anyhow.

Mr. DIFFIE. Whether it is desirable or not, it is perfectly infeasible. But that both the original 1970s, 1980s DOD objective of building an operating system that could maintain what the Soviets called *praksa*; prison laboratories, where they didn't have to trust the staff because they weren't going to let them go anywhere. Or at standpoint in Java we call sandbox or at the other end improving software development methodology, which will have a profound impact not only in security but through all of our economy. I think both of these things will play a role.

Mr. IANNA. I think there are—as a service provider who uses a lot of these different types of hardware and software technology, either in the provision of service directly or the support systems that help us provision and maintain these services, we have a practice where we try to test the software in our laboratory and attempt—and I do use the word “attempt”—to simulate many of the conditions that we may find in the network before the software and the hardware is introduced into the network. It is called an integrated test network.

Some vendors find that process very, very cumbersome. It does add time to our development process and our deployment of technology.

But the alternative is to have software out there which may have an interaction with some other software out there which creates something that is very bad for your customers on your network.

I would like to be able to say that we find every bug in every software issue that we have and we know of every interaction that is bad that can happen out there, that is not the case. But we do have—and we have shared practices in the telcom ISAC and, the NRIC, on ways of testing those things.

By the way, it was interesting, at least what I was thinking about this issue, one of the interesting things here is we had a time in our recent history where we had to do this very quickly, because we didn't have all the time in the world, and that was for Y2K. We had a date certain that we had to do something.

And we picked a way of doing it because we couldn't make all the permutations, so we shared a lot of information. And if I knew this software interacting with this switch with this operating system was okay by some other vendor's test, I accepted that and I shared my tests with somebody else too. Otherwise, you would have, you know, even if you took one second for every test in the

3 years, you wouldn't have been able to test all the permutations. And that worked extremely well.

The difficulty we have in this situation is we don't have a date certain when something is going to happen. And we don't know—the thing that might happen is not defined and will change. And creating that sense of urgency around that I think is important for us at the government level and at the industry level to do that we must be cyber secure and we must take this very seriously. We do only because we have had failures where software was the cause.

Ms. GAU. Fortunately, at this point, we have not suffered a large-scale cyber attack by a foreign government or foreign agents so to speak. But AOL, as I mentioned, experiences hacker attacks on a daily basis. And over the years, we have found that that kind of pounding of our systems has helped us identify security problems that we are then able to fix. Because as it turns out, the hacker in question was just a teenager working, you know, on the computer, or not working, but playing on the computer in the home, and wasn't really seeking to do anything but to gain bragging rights for having accomplished something.

And obviously, not everyone can do that to every product that they are going to put out into the market. There is only so much beta testing you can do. But one of the things that we have done with vendors of ours, particularly, for example, companies that participate in the shopping area on AOL, what we consider certified merchants. We require them to undergo security audit with one of two firms that we identify to them.

Now, on a large-scale basis, that is not realistic, because there are costs involved. And so only the big players can really come to the table if they want to be in the shopping area on AOL because they are going to have to pay for this security audit.

But there is no question that stress-testing of systems and perhaps further R&D, as well as further incubation periods for products might lead in a direction where we have less products in the market place that you have security holes discovered in once they hit consumers.

Ms. LOFGREN. Mr. Chairman, we should let them have lunch.

Mr. THORNBERRY. I think the gentlelady's point is well taken.

Let me thank each of you again for your time and your contribution. Let me also invite each of you to continue to discuss these issues with the members and the staff of this subcommittee.

As we move ahead, we are going to continue to need your input and our suggestions.

For example, next week we are having this hearing on research and development. What areas do you think the federal government should concentrate its research and development in the area of cybersecurity? If you have thoughts on that, we would like to hear it.

Again, thank you for being here.

And this hearing stands adjourned.

[Whereupon, at 1:16 p.m., the subcommittee was adjourned.]

## APPENDIX

## MATERIAL SUBMITTED FOR THE RECORD

## RESPONSES TO QUESTIONS FOR THE RECORD FROM DELL, DR. JAMES CRAIG LOWERY

1. There has been widespread concern among computer industry insiders that DHS is not taking information security vulnerabilities seriously enough. There is still no Undersecretary for Information Analysis and Infrastructure Protection, and even when one is in place, there is concern that information security will be relegated to second-class status. Industry has expressed the interest in expanding partnerships with government agencies to improve security, but DHS does not appear to be moving quickly to embrace this idea.

**a. What do you see as the government's role in increasing security and standards setting? Could it be fostered through partnerships (such as those done through National Institute for Standards and Technology) and purchasing criteria? Would government mandated standards, such as the Common. Criteria, be a helpful baseline or a hindrance to future innovation?**

**Response:** Dell is interested in sharing its insights and views on cybersecurity with the Department of Homeland Security. Overall, the government's role in increasing security and standards setting is as a customer and through its participation in organizations such as the Center for Internet Security in an open, voluntary and consensus-based process that includes input from all stakeholders.

Security is a moving target, and the products and services addressing security needs necessarily evolve as the landscape changes. Government mandated standards would likely result in a one-size fits-all approach that fails to address the security problem and would also be an obstacle to innovation in our industry. Additionally, there is some concern that the process associated with the setting of government standards would be slow and cumbersome that technology and knowledge would always be ahead of government standards.

**b. From what you can tell, is there sufficient information-sharing taking place between researchers who discover most vulnerabilities, companies who created the products and DHS? If CERT were formally connected to DHS, would that help FedCIRC with information dissemination and the remediation of security problems and breaches?**

**Response:** We support the information-sharing that is taking place with organizations such as CERT Coordination Center, the SANS Institute, the Center for Internet Security, and the Free Standards group. These organizations are working to develop security solutions based on consensus and standards with the input from government agencies, businesses, universities, and individual security experts and to disseminate information. In order for these organizations to remain effective, it is important for Federal departments such as the Department of Homeland Security to participate in these organizations.

**c. How can the government help companies be more responsive to known security issues? Would a law providing safe-harbor, with a sunset, help encourage companies to quickly fix security issues after they are discovered?**

**Response:** The Federal Government should provide information on its cybersecurity needs to its vendors as well as provide its input and views to organizations that are engaged in an open, voluntary and consensus-based process for the development of security standards.

## RESPONSES TO QUESTIONS FOR THE RECORD FROM EQUINIX, MR. JAY ADELSON

1. There has been widespread concern among computer industry insiders that DHS is not taking information security vulnerabilities seriously enough. There is still no Undersecretary for Information Analysis and Infrastructure Protection, and even when one is in place, there is concern that information security will be relegated to second-class status. Industry has expressed the interest in expanding partnerships with government agencies to improve security, but DHS does not appear to be moving quickly to embrace this idea.

**a. What do you see as the government's role in increasing security and standards setting? Could it be fostered through partnerships (such as those gone through National Institute for Standards and Technology) and purchasing criteria? Would government mandated standards, such**

**as the Common Criteria, be a helpful baseline or a hindrance to future innovation?**

**Response:** The government has an opportunity to assume a leadership position in the coordination of efforts to create common security standards. While like many voluntary standards, they do not require regulatory enforcement such standards can be useful as competitive differentiators and therefore industry-driven.

Partnerships would be required to fulfill this need, as currently the federal, government does not have the background, and relationships required on an international level to begin this dialogue. It would be of tremendous benefit to the industry if this could change, and via the UnderSecretary for Information Analysis and Infrastructure Protection, such expertise could be established within the DHS over time.

The government has had a role in developing cyber and physical security best practices through the FCC's Network Reliability and Interoperability Counsel (NRIC), which can provide a model and a starting point. However, in our opinion, NRIC is not an effective place to create these best practices going forward, as it only represents regulated entities, a small subset of Internet infrastructure. Migrating the homeland security best practices work from NRIC to DHS will allow the scope of that work to be expanded to include previously untapped communities and a better representation of Internet infrastructure in general.

Purchasing criteria to meet certain standards, as well as process and technology criteria, would be inclusive in these standards. While it would be appropriate for the federal government to act as an early adopter of these Common Criteria, the purchasing power of government does not alone constitute a significant enough motivator to catalyze adoption of these standards.

**b. From what you can tell, is there sufficient information-sharing taking place between researchers who discover most vulnerabilities, companies who created the products and DHS? If CERT were formally connected to DHS, would that help FedCIRC with information dissemination and the remediation of security problems and breaches?**

**Response:** Our visibility into the information-sharing between DHS and other entities is limited. Certainly, at an operational level, we have seen no indication that DHS has had any significant communication with elements of the industry that represent the Internet infrastructure, outside of the major router manufacturers and the top five telecommunication carriers. While five years ago this may have been sufficient, the Internet infrastructure has evolved into tens of thousands of individual influential entities that all require significant communication from DHS in the event of a crisis or in crisis preparation. CERT need not be formally connected to DHS for CERT's information to be better propagated. The communications path between DHS and industry can potentially be better funded and maintained than the communication path between CERT and industry, and this neutral organized approach could incorporate other information outside of CERT in the decision-making process of who to tell what information.

In sharp contrast to DHS' current communication practice with industry, informal industry-based communication practice is strong between similar service providers, such as ISPs and telecom carriers, outside of any ISACs. Unfortunately, enterprises and large content providers have been excluded from this self-developed communication due to their relative infancy in the Internet infrastructure, and therefore this provides an excellent opportunity for DHS to develop these practices, particularly amongst the largest population of Internet infrastructure businesses represented by enterprise and content.

**c. How can the government help companies be more responsive to known security issues? Would a law providing safe-harbor, with a sunset, help encourage companies to quickly fix security issues after they are discovered?**

**Response:** Current communication plans from government to industry are event-driven. A major restructuring of this concept for the Internet industry would be necessary, shifting the approach to scheduled communication in addition to event-driven communication. The nature of business revenue priority would typically defocus enterprises from maintaining up-to-date information, however government-approved standards, that require regular participation by enterprise, would ensure proper communication practice.

Laws providing safe-harbor would appropriately address privacy concerns. In essence, laws that protect service providers from brand damage after an event, such as exemptions from the Freedom of Information Act, would be necessary to ensure two-way communication.

## RESPONSES TO QUESTIONS FOR THE RECORD FROM AT&amp;T, MR. FRANK IANNA

1. There has been widespread concern among computer industry insiders that DHS is not taking information security vulnerabilities seriously enough. There is still no Undersecretary for Information Analysis and Infrastructure Protection, and even when one is in place, there is concern that information security will be relegated to second-class status. Industry has expressed the interest in expanding partnerships with government agencies to improve security, but DHS does not appear to be moving quickly to embrace this idea.

**a. What do you see as the government's role in increasing security and standards setting? Could it be fostered through partnerships (such as those done through National Institute for Standards and Technology) and purchasing criteria? Would government mandated standards, such as the Common Criteria, be a helpful baseline or a hindrance to future innovation?**

**Response:** Government should first ensure that its procurement activities across Federal, State, and Local settings are properly coordinated through a common set of security standards. This is a logical first step for our nation—and frankly, unless such coordination can occur between these separate government entities, it will be unlikely to occur in a more diverse commercial setting. Selection of which standard to use is not the critical issue; security best practices are well understood and agreed upon by current security professionals. The more important issue is that the selected standard be uniformly applied—and government procurement is the obvious place to start.

**b. From what you can tell, is there sufficient information-sharing taking place between researchers who discover most vulnerabilities, companies who created the products and DHS? If CERT were formally connected to DHS, would that help FedCIRC with information dissemination and the remediation of security problems and breaches?**

**Response:** Information sharing about vulnerabilities has certainly gotten much better and companies like AT&T are taking advantage of that information to better protect against and respond to vulnerabilities as they are identified. For example, information shared quickly during the recent slammer and blaster events helped AT&T take the necessary assessment and remediation actions that much more efficiently and effectively. Regarding CERT specifically, what is most important is that CERT be among the resources available to DHS as part of the overall public-private partnership for information-sharing purposes. It seems unnecessary for CERT to be “formally connected” to DHS in order for it to continue to be a valuable tool for DHS and the private sector alike. The much more urgent issue is the prevention and removal of vulnerabilities from commonly used products such as commercial operating systems and applications.

**c. How can the government help companies be more responsive to known security issues? Would a law providing safe-harbor, with a sunset, help encourage companies to quickly fix security issues after they are discovered?**

**Response:** Government should foster a competitive commercial environment in which marketplace forces reward products and services that are free of security vulnerabilities. One area in which this can occur relates to government procurement (see above); another relates to a renewed assessment of the proper assignment of liabilities should such vulnerabilities result in business losses for users. That said, it is also important to ensure that companies that act responsibly by identifying vulnerabilities through timely and prudent evaluation, by notifying its customers and by otherwise handling identified flaws in a responsible manner are protected from liability and thus not discouraged from acting responsibly.

2. Several experts have cited the threat of cyber attacks by well-organized and technically savvy terrorist groups—specifically Al Qaeda. An article in the Washington Post last year laid out chilling scenarios in which terrorists might carry out cyber attacks that could do the same amount of damage to our critical infrastructure as tons of explosives. Another fear is the coordination of a cyber and physical attack, so that our response capabilities would be compromised or even shut down just when we need them most.

**a. Do you agree that these threats are real? If so, how much of a priority should they be? Are there other variations of the cyber threat that should be getting more attention than they have?**

**Response:** It is difficult for an individual private-sector entity such as AT&T to assess the degree of actual cyber-threats, especially those outside of the telecommuni-

cations industry, and Congress should look to government intelligence agencies, and not the private sector, to gauge the likelihood and severity of cyber-threats. Nonetheless, the increase of attempted intrusions and disruptions that we have identified over time does suggest that there are real threats, and addressing these threats continues to be a high priority for AT&T, and should be for companies within each critical industry sector. Like the FCC/NRIC model, each industry sector should work together to identify the critical systems that could be exploited to cause disruptions, and develop and observe voluntary best practices to improve each company's intrusion detection, deterrence and disaster recovery capabilities. This assessment must be done separately for each sector, and specifically for each mission-critical system at the "micro" and not "macro" level to be sure that characteristics unique to each system are identified and evaluated. Furthermore, each sector should develop measures around these best practices so that each industry's progress can be measured over time. In addition, it is important for companies that own and operate critical infrastructures, such as AT&T, to have ongoing communications with government intelligence entities to stay informed as new threats are identified.

**b. Are we, and specifically is DHS, doing enough now to address the possibility of large-scale cyber attacks? If not, what more needs to be done—is it a question of changing priorities? hiring additional personnel? placing a higher-ranking official in charge of the cybersecurity issue?**

**Response:** The Department of Homeland Security was only created in March of this year, making it nearly impossible for a private-sector corporation such as AT&T to fairly assess its effectiveness in addressing cyber-security. Certainly more can be done, and naming a senior official responsible for cybersecurity will help.

**c. What is being done to research or combat the possibility of viruses, worms or other cyber threats morphing, so that they are impossible to protect against?**

**Response:** The global cyber community is currently investing countless hours and resources in the establishment of incident response teams that identify and respond to viruses, worms, and other cyber attacks. While this is appropriate given our current global cyber security posture, such security investment could be redirected toward alternate innovations that could help enable new services and hence drive the economy. As such, the primary research issue should involve the prevention and removal of security vulnerabilities from occurring in the first place. This must start with the vendors of software products that are used almost ubiquitously across the globe on servers, workstations, and other devices. Virtually every major security incident being experienced in recent months rely on the presence of such software vulnerabilities.

**d. From what you can tell, is there sufficient information-sharing taking place between the intelligence community (and specifically the DHS Intelligence Analysis Directorate), which analyzes threats, and the science and technology arena (and specifically the Science and Technology Directorate), where new solutions and tools can be developed to counteract the most likely or most worrisome threats?**

**Response:** The private sector is not in a position to assess the quality of information sharing between these two nascent directorates within DHS.

**e. Do you feel the Information Sharing Analysis Center (ISAC) established under Presidential Order is the right structure for information sharing between sectors and the federal government? What would you recommend as an optimal model for ISAC-like activities? How is DHS working with your industry ISAC?**

**Response:** We agree with the ISAC concept but would suggest that there is no single model that would meet the needs of every critical infrastructure. Infrastructure operators in some sectors, such as telecommunications, have a compelling need to communicate frequently through multiple points of interface. This is because the components, or segments, of the telecommunications infrastructure as interconnected and the functioning of each segment has significant implications for other operators. These communications channels are frequently exercised because incident management in the telecommunications industry is a daily necessity, due to the widely dispersed assets, which are exposed to a multitude of threats. Other infrastructures, such as electric power, probably have a similar requirement. However, an infrastructure such as water, likely does not have the same need for many operators to communicate with one another on a regular basis.

For infrastructures such as telecommunications, we believe the National Coordinating Center (NCC), operated by the National Communications System (NCS),

which is a component of DHS, is the best model. It was established in 1984 and has functioned as an “ISAC” for over twenty years. The federal government operates the center while the private sector provides representatives for “resident” and “non-resident” memberships. The NCC is the focal point for coordination of disaster response for telecommunications under the Federal Response Plan (FRP). Government funding and participation in this ISAC makes a compelling business case for participation by the private sector.

**f. How has the insurance industry reacted to the development of cyber attacks and cyber terrorism as a risk factor for your industry? Are losses caused as a result of such incidents generally covered under existing policies, or have new products been created to specifically address this risk factor? Do you have any sense of the impacts on insurance costs?**

**Response:** The insurance industry has begun to develop new insurance products albeit this market is in the formative stages. Losses caused by cyber-related terrorist acts are generally not covered under existing policies. Though some new insurance products have become available, few insurance companies are willing to take on such risk, and even where available, coverage is limited and costly. There has been no impact to our insurance costs because this risk is excluded from our policies. If we chose to purchase insurance that protected against loss from this risk our insurance costs would increase.

**3. Providing patches to vulnerabilities is time and resource intensive. How does your company address the problem of legacy equipment and software with respect to cybersecurity? Are older and discontinued products supported with respect to fixing newly discovered security flaws? If so, how is the end user notified? Is there a role for the federal government in this process?**

**Response:** This is a significant and costly issue from a cybersecurity perspective. In many cases, security patches are not provided to address flaws in legacy systems and software, and we are left with no choice but to replace potentially vulnerable but otherwise operational capabilities. For example, commercial operating systems are often periodically “retired”, at which point vendors will no longer provide remediation, patches or support. Entities running those operating systems have no option but to replace them or risk the possibility that vulnerabilities could be exploited.

4. Up to this point, cybersecurity has depended on voluntary consensus across industry. The Federal Communications Commission (FCC) has a process via the National Reliability and Interoperability Council (NRIC) that seems to have worked for the telecommunications sector, but much of this was based on the FCC regulatory role for that industry.

**a. Could DHS fill this void for establishing best practices, common criteria, and standards for Information Technology products and services, particularly for the Internet? If so, how might that be structured?**

**Response:** With regard to telecommunications, the Network Reliability and Interoperability Council, established in the early 1990’s, has developed best practices for the wireline communications industry for reliability, physical and cyber security, etc., and the NRIC has expanded its work in the last few years on best practices to address IP-based, wireless and cable services. The Council has also established processes for standards and for templates (criteria) for interconnection and interoperability. Therefore, we do not see a void with regard to telecommunications. DHS should be encouraged to interact with the FCC/NRIC with regard to telecommunications best practices. This model could be used by other sectors as well, but each sector should be responsible for working with the appropriate government agencies (e.g. perhaps DOE and FERC for the electric power industry, Treasury and the Federal Reserve for the financial services industry), in conjunction with DHS, to develop and implement best practices tailored to each specific sector.

**b. Are there aspects of standards for which a mandatory approach might be more appropriate, as is the case, for example, in health care or telecommunications?**

**Response:** The standards process is a necessary part of the service industry. In telecommunications, standards are essential because suppliers and competitors are all interconnected using ubiquitous standards agreed to by the industry. Service industry participants work the standards process in various standards committees such as ATIS and IETF for the telecommunications industry. The benefit of the standards process to the industry is the ability to gain consensus by all participants. This ensures that all “voices” are heard from and one group does not dominate the process. ANSI provides for accreditation to ensure that standards committees do fol-

low this procedure. (if they are certified). However, a mandatory approach to security standards would be extremely difficult, and participation may be in jeopardy since industry participants will have concerns and the open exchange of information will not be as forth coming. Rather than attempting to mandate security standards, a better approach is to use an NRIC-like approach (described further in 2(a) and 4(a) above) and allow peer performance pressure to be the stimulus for improvement in the market throughout each sector.

**c. Some major auditing firms want to help companies assess their security vulnerabilities and develop plans to address them. How is the business case being formed to justify the additional costs?**

**Response:** Business Continuity is an essential process for each enterprise. Each enterprise does some degree of Business Continuity and risk assessment/remediation. This risk assessment must examine closely the “expected value” of each security investment, because even though the probability of loss is low, the impact could potentially be quite high. This analysis is key in order to establish accurate priorities in where to invest limited security resources. The use of external auditing firms helps the enterprise with their business continuity process. Use of auditing can be for: validation of internal risk assessment, identification of gaps, new opportunities or thoughts processes, certification of center operations, etc.

The business case for auditors would be part of the business continuity business case.

5. Emergency preparedness and disaster recovery are common themes for the physical infrastructure, but there does not appear to be adequate attention to these areas for cyberspace.

**a. From the perspective of your industry, how should the Department of Homeland Security prioritize its cybersecurity activities, from threat detection through disaster recovery?**

**Response:** Priority one should involve remediating vulnerabilities in software that powers our critical infrastructure. Investments in software engineering process improvements, research into better tools for ensuring correctness of software, and increased attention to correctness in government procurement activities should be paramount in the DHS plans.

In addition, DHS alone cannot achieve the charter of the department. It will take partnership with the industry to develop the priorities and programs to meet the demands of the “new” cyber world we all live in now. Any major initiative that could have a significant impact on private sector infrastructures should include, from the outset, industry participation, guidance and expertise. For example, much has been said about the possibility that the government might establish a center for cyberspace security. However, before undertaking such an important project, government and industry need to work together to explore whether we should have a national center for cyber space security or not, and if so, who would participate, and how it would operate.

**b. What should be the threshold for federal involvement in the event of a cyber attack? When should it be left entirely to the private sector to respond?**

**Response:** While the majority of critical infrastructure is owned and operated commercially, a non-trivial percentage (15% by most estimates) is controlled by government. Accordingly, government must ensure that it is properly responding to cyber attacks for these resources. Leading by example may be the most powerful means for improving the overall security posture of the nation.

In addition, thresholds for determining when federal government should get involved should be established on a sector-specific basis. In telecommunications, thresholds have been defined through the NS/EP process and the work of the NCC/NCS. Each event is different and it is difficult to define what the threshold should be to capture a process that would be applicable to all events. In the cyber world, each event has unique characteristics and it is difficult to define what is the critical nature of the event. The NCC/NCS has a long history in knowing when to pull the service providers together for a common restoration. Many of the principles applied over the years to the telecommunications structure can be transferred to the cyber arena. The NSEP process should be adopted for these purposes. These principles can and should be applied to other sectors, and adjusted for each sector that reflect the needs and particular characteristics of that sector. In fact, the threshold could be different in each industry sector.

**c. What role could the federal government play in reconstituting Internet service if a major debilitating attack were to occur?**

**Response:** To the degree that government-controlled infrastructure is included in the overall Internet community (e.g., NIPRnet, DISN, FTS-2001, etc.), government should obviously take the lead in coordinating proper reconstitution of such resources with its vendors, suppliers, and partners. More importantly, government should try to take the lead in preventing such attacks from occurring through the software vulnerability reduction measures outlined above.

In addition, the government should look to the NCC/NCS, established in 1984 with the break up of the Bell System, to coordinate communications restoration when appropriate. Over the years the NCC has expanded its membership from traditional circuit switched providers to internet-related providers and vendors. In fact, during the September 11th event, the NCC, with its links to the White House, worked with industry to restore Wall Street first as part of the recovery. Continued use of the NCC/NCS in the "trusted" environment is the best way for the recovery process to work when required.

**d. In the event of a major cyber attack, what are your concerns with respect to disaster recovery for your company and more broadly? Do you think that existing continuity and recovery planning are sufficient? If not, what more needs to be done?**

**Response:** AT&T has the premier physical Disaster Recovery capability in the industry, which addresses the physical replacement of destroyed assets. AT&T has invested over \$300M in infrastructure and processes that can be deployed to recover from such a disaster scenario. In addition, AT&T has detailed business continuity and recovery plans for all of our key data centers and systems. These processes are exercised regularly and overseen by resiliency experts at AT&T Labs to ensure that plans are tested and refreshed as warranted. We also monitor the health of our networks constantly and can identify and address abnormalities very quickly. Even in these tight economic times, AT&T has continued to invest including expanding our disaster recovery capabilities to our key facilities outside the United States. It is important for all entities, but especially operators of critical infrastructures, to perform periodic and rigorous assessments of their mission-critical functions to minimize the impact that disruptions might otherwise cause.

With regard to recovery from a major cyber attack, disaster response could take many forms. There are basic principles to guide the recovery: first, the detection and analysis of traffic data anomalies and other indicia in real-time; and second: remediation actions, which could range from applying software patches and upgrades, to quarantining and inoculating infected LANs, to shutting off routers to prevent further damage and rebooting machines using "clean" saved software.

**e. Is there a need for a coordinated international response as part of the efforts to protect national information infrastructures? What form might this response take?**

**Response:** Obviously, global coordination is required. Multinational corporations do this across their business unit structure, often in a seamless manner. In addition, the international environment is critical to controlling the health of the Internet. From a disaster recovery viewpoint, AT&T is investing in recovery for service nodes in Europe.

Our Business Continuity and Risk Assessment processes are currently being refreshed in light of changed conditions. Establishing a working group across national boundaries could have benefit just as the NRIC Council has provided benefits in the communications industry. Cyber attacks can come from anywhere, therefore international cooperation at both the government and industry levels is a necessary component. However, currently, it is be very difficult for the private sector to engage in effective information-sharing and security coordination efforts in a global context because there are so many different approaches to information protection and disclosure world-wide at this time. There is a critical role for the U.S. government to play in structuring this partnership to ensure that U.S. corporations and citizens are protected by U.S. laws. Active private sector participation requires significant harmonization to ensure adequate legal protections such as protection of sensitive information are continually maintained.

#### RESPONSE TO QUESTIONS FOR THE RECORD FROM AOL, MS. TATIANA GAU

1. There has been widespread concern among computer industry insiders that DHS is not taking information security vulnerabilities seriously enough. There is still no UnderSecretary for Information Analysis and Infrastructure Protection, and even when one is in place, there is concern that information security will be relegated to second-class status; Industry has expressed the interest in expanding partner-

ships with government agencies to improve security; but DHS does not appear to be moving quickly to embrace this idea.

**a. What do you see the government's role in increasing security and standards setting? Could it be fostered through partnerships (such as those done through National Institute for Standards and Technology) and purchasing criteria? Would government mandated standards, such as the Common Criteria, be a helpful baseline or a hindrance to future innovation?**

**Response:** We believe that government's role is to lead by example on cybersecurity, to encourage information sharing and the development of industry best practices; support R&D, and to enter into partnerships with industry to improve cybersecurity in areas where it is lacking. Because cybersecurity is such a rapidly evolving area we do not believe that government mandated standards are a particularly effective approach, as such standards could quickly become obsolete. However, we do think that government procurement standards may be helpful in encouraging best practices throughout the private sector.

**b. From what you can tell, is there sufficient information-sharing taking place between researchers who discover most vulnerabilities, companies who created the products and DHS? If CERT were formally connected to DHS, would that help FedCIRC with information dissemination and the remediation of security problems and breaches?**

**Response:** To our knowledge, while there is a good deal of information-sharing taking place among researchers and IT companies, there is not yet significant information-sharing between DHS and the ISP sector. We applaud the recent decision by DHS to create a government CERT that will coordinate with the private sector. We believe such a collaborative approach will create an environment that is conducive to information-sharing and cooperation.

**c. How can the government help companies be more responsive to known security issues? Would a law providing safe-harbor, with a sunset, help encourage companies to quickly fix security issues after they are discovered?**

**Response:** AOL and other industry leaders already spend very significant sums of money on cybersecurity. However, government can foster greater responsiveness to known security issues through information-sharing, and by educating the public about security issues, as AOL does through its service. Government can play a particularly important role by providing easy-to-access security warnings for small business and home users.

#### RESPONSES TO QUESTIONS FOR THE RECORD FROM MICROSOFT, MR. PHIL REITINGER

1. There has been widespread concern among computer industry insiders that DHS is not taking information security vulnerabilities seriously enough. There is still no UnderSecretary for Information Analysis and Infrastructure Protection, and even when one is in place, there is concern that information security will be relegated to second-class status. Industry has expressed the Interest in expanding partnerships with government agencies improve security, but DHS does not appear to be moving quickly to embrace this idea.

**a. What do you see as the government's role in increasing security and standards setting? Could it be fostered through partnerships (such as those done through National Institute for Standards and Technology) and purchasing criteria? Would government mandated standards, such as the Common Criteria, be a helpful baseline or a hindrance to future innovation?**

**Response:** The government has a vital and tailored role to play in cyber security. First and foremost, the United States Government is the owner and operator of some of the largest and most sensitive computer networks in the world—its actions regarding its own cyber security can serve to demonstrate both the importance of the problem and best-in-breed solutions. Accordingly, the U.S. Government must act as a model, buying technology engineered for security, and implementing state-of-the-art security practices.

Second, the U.S. Government must attack the "knowledge gap" regarding cyber security—even today we do not know the quantitative risks posed by a lack of cyber security, and in which areas public and private actions fall short of addressing these risks. Business leaders are very good at risk management, but some of the risks posed by cyber crime and cyber attack are best known to the Government and need

to be shared, to the greatest extent possible, with the private sector. This will enhance the business case for cyber security to the benefit of all. In particular, we all need to know more about interdependency between sectors and how that may affect our economy and our nation. Moreover, even with the increasing business focus on cyber security and enhanced private sector action, in some areas there may be a national or homeland security need for computer and network security above what the market will provide. Therefore, the government, with knowledge of the risk in hand and recognizing the dynamic nature of the problem, needs to conduct an analysis of where private action may fall short and then determine the best way to address this shortfall through tailored action.

Third, the U.S. Government needs to otherwise catalyze and enhance private action. There is and has been considerable activity in the cyber security realm, which can lead to two contrary but related mistakes. The first is to think that all, this activity is progress, and that the cyber security problem is close to being solved. The second is to view this activity as mere churn without progress. In fact, considerable progress has been made, with the private sector increasingly focusing on and devoting resources to cyber security, and the public sector taking actions such as creating the Department of Homeland Security and adopting an improved information security governance structure through the enactment of the Federal Information Security Management Act. The federal government is uniquely able to continue and enhance this progress. It can help reduce the “churn” by examining the activity that is taking place and identifying and supporting the private and public initiatives that offer the best opportunity to solve problems. It can, help to develop and support metrics by which the private sector can judge its status and capabilities. As identified in my testimony, the federal government should provide more support for cyber security R&D (among the topics could be improved development tools, security for Internet-scale computing, human-computer interaction and security, priority routing, basic protocol research, and wireless security). And with respect to information sharing, besides sharing its own information (*see above*), the federal government can catalyze information sharing by the private sector by working with it to develop interfaces and protocols for sharing information among the various players and for the subsequent protection and use of that information—this would help to ease the burden of sharing information and increase the trust that shared information would be handled appropriately.

Fourth, the U.S. Government must fulfill its particular responsibilities as a national government, including for national and homeland security. These include continuing to enhance the capability of law enforcement to catch and punish cyber criminals, because without an effective deterrent the amount of cyber crime will continue to grow. The Government can also raise public awareness about computer security, and build international relationships and agreements that enhance computer security worldwide.

The government role in standards setting is also vital if properly tailored—in our view, the market should drive the emergence of open standards. If market competition is permitted to determine which standards succeed, users are most likely to get the best mix of security and value, while the process itself will ensure that more secure standards constantly replace those that are less secure. That said, the government can and should set the requirements for its IT purchases, relying to the greatest extent possible on the standards developed, through market-driven means. This gives the government the benefit of widely interoperable and more up-to-date technology and processes.

Moreover, as your question also suggests, where appropriate the government’s acquisition policies should include purchasing software whose security has been evaluated and certified under the internationally-recognized (and U.S. supported) Common Criteria for Information Technology Security. Policies requiring the acquisition of software that has received appropriate Common Criteria certifications should be developed and applied consistently and evenhandedly, and we applaud DoD’s recent efforts to make clear that its security policies apply to software that has been developed under all business, development, and licensing models. Such efforts to procure only security-engineered technology, and specifically such clear support for the Common Criteria, will help strengthen the government infrastructure and motivate markets.

The government should, however, avoid mandating standards for use by the private sector. Legislated standards are likely to become quickly outmoded—indeed, they may be outmoded at enactment. Standards are already “following” rather than “leading,” that is, standards tend to enshrine best current practice rather than encapsulate expected innovation. Adopting a particular standard in legislation or regulation may enshrine outdated and antiquated technology and practice on our most

critical infrastructures. Mandatory standards can also restrict innovation, by reducing the benefit from developing new technology or practices that are non-compliant, and also skew innovation, by favoring one technology or practice over another. Finally, mandating standards can actually drive security to a floor. Here, as elsewhere, the government must tailor its activity to meet specific needs, and act in the least intrusive manner possible, to avoid damaging the market's continuing innovation.

**b. From What you can tell, is there sufficient information-sharing taking place between researchers who discover most vulnerabilities, companies who created the products and DHS? If CERT were formally connected to DHS, would that help FedCIRC with information dissemination and the remediation of security problems and breaches?**

**Response:** Information sharing regarding vulnerabilities is certainly taking place, and of course I would like to see it improve. Responsible disclosure of vulnerabilities minimizes risk to users, the

Internet, and the critical infrastructures that depend upon it by giving vendors an opportunity to develop a fix for a vulnerability before giving attackers the knowledge necessary to launch attacks. Microsoft applauds and thanks those researchers who follow responsible disclosure policies.

Therefore, Microsoft is working with other industry leaders to propose and institutionalize industry best practices for handling security vulnerabilities in ways that more effectively protect Internet users. We are a founding member of the Organization for Internet Safety (OIS), an alliance of leading technology vendors, security researchers, and consultants that is dedicated to the principle that security researchers and vendors should follow common processes and best practices to efficiently resolve security issues and to ensure that Internet users are protected. See [www.oisafety.org](http://www.oisafety.org). Last month, OIS published a set of best practices for reporting and responding to security vulnerabilities. These guidelines, which were built with input from across the security community, provide specific, prescriptive guidance that establishes a framework in which researchers and vendors can work together to improve the speed and quality of investigations into security vulnerabilities, then jointly provide guidance to help users protect themselves and their infrastructures. We view these best practices as an important step in elevating standards for accountability on all fronts and among all audiences in managing security vulnerabilities.

With regard to the formal connection of CERT to DHS, I would need further information on how such a proposal would work before commenting in detail.

**c. How can the government help companies be more responsive to known security issues? Would a law providing safe-harbor, with a sunset, help encourage companies to quickly fix security issues after they are discovered?**

**Response:** The U.S. Government can help companies be more responsive to known security issues by taking the actions described above—being a leader and securing its own systems, addressing the knowledge gap, catalyzing and enhancing private sector activity, and fulfilling its governmental responsibilities. In particular, addressing the knowledge gap will help business both to make rational decisions about cyber security and risk management and to implement the best defense.

As for your question about Safe Harbor, I would need more information about the proposal to comment.

